2019

Directive to the members of ICPAC on Anti-Money Laundering and Combating Terrorist Financing Activities

pursuant to Section 59(4) of The Prevention and Suppression of Money Laundering and Terrorist Financing Law of 2007 188(I)2007 as amended in 2010, 2012, 2013, 2014, 2016 and 2018 by Laws 58(I)/2010, 80(I)/2012, 192(I)/2012, 101(I)/2013, 184(I)/2014, 18(I)/2016, 13(I)/2018, 158(I)/2018 and 81(I)/2019

The Institute of Certified Public Accountants of Cyprus

Preface

This Directive is issued by the Council of the Institute of Certified Public Accountants of Cyprus in its capacity as a competent authority pursuant to (a) the Decision 53.300 of the Council of Ministers of the Republic of Cyprus on March 7, 2001 and (b) the Prevention and Suppression of Money Laundering and Terrorist Financing Law of 2007, as amended up and until ~~2018~~ 2019, (articles 59(1)(d) and 59(4)), hereafter referred to as the "Law".

The Law, being in line with the Directive EU 2015/849 of the European Parliament and of the Council of 20 May 2015, stipulates the obligations and responsibilities for implementation by professionals, of measures against money laundering and combating the financing of terrorism.

This Directive deals with the statutory and professional requirements in relation to the prevention, recognition and reporting of money laundering and terrorist financing activities.

In the preparation of this Directive, consideration was given to the Cyprus National Assessment of Money Laundering and Terrorist Financing Risks report dated October 2018, the report from the Commission to the European Parliament and the Council on the assessment of the risks of money laundering and terrorist financing affecting the internal market and relating to cross-border activities dated June 2017, Financial Action Task Force (FATF) Recommendations, the Professional Money Laundering report issued by FATF dated July 2018 as well as the Risk-based Approach Guidance issued by FATF in June 2008 for Accountants and for Trust and Company Service Providers. The International Monetary Fund staff recommendations emanating from their "Risk-based Analysis of Cyprus Anti-money Laundering Regime" report dated 10 October 2012 and the latest post-programme discussions dated June 2018, were also taken into consideration.

The present Directive replaces the '*Prevention and Suppression of Money Laundering Activities'* Directive to the members of ICPAC, issued by the Council of the Institute in September 2013.

June 2019

Table of Contents

1. Introductory provisions and definitions

1.1 Definitions

1.1.1 Some of the basic terms used throughout this Directive are defined as follows:

Beneficial Owner Any natural person who ultimately owns or controls the client and/or the natural person on whose behalf a transaction or activity is being conducted and includes at least:

(A) in case of corporate entities:

(i) the natural person who ultimately owns or controls a corporate entity through direct or indirect ownership of a sufficient percentage of the shares or voting rights or ownership interest in that corporate entity, including through bearer shareholdings, or through control via other means, other than a company listed on a regulated market that is subject to disclosure requirements consistent with European Union law or subject to equivalent international standards which ensure adequate transparency of ownership information.

Provided that:

(a) an indication of direct shareholding, shall be a shareholding of 25% plus one share or an ownership interest of more than 25% in the corporate entity, held by a natural person, and

(b) an indication of indirect ownership shall be a shareholding of 25% plus one share or an ownership interest of more than 25% in the client held by a corporate entity, which is under the control of a natural person, or by multiple corporate entities, which are under the control of the same natural person or persons.

Provided further that the control by other means can be verified, inter alia, based on the criteria provided for in section 142 (1) (b) and section 148 of the Companies Law,

(ii) the natural person who holds the position of senior managing official if, after having exhausted all possible means and provided there are no grounds for suspicion, no person under sub paragraph (i) of the present paragraph is identified, or if there is any doubt that the person identified is the beneficial owner.

Provided that records of the actions taken in order to identify the beneficial ownership under sub paragraphs (i) and (ii) above are well documented.

(B) in case of trusts:

(i) the settlor,
(ii) the trustee or commissioner,
(iii) the protector, if any,
(iv) the beneficiary, or where the individual benefiting from the legal arrangement or legal entity have yet to be determined, the class of persons in whose main interest the legal arrangement or entity is set up or operates,
(v) any other natural person exercising ultimate control over the trust by means of direct or indirect ownership or by other means, and

(C) in the case of legal entities, such as foundations, and legal arrangements similar to trusts, the natural person holding equivalent or similar positions to the person referred to in paragraph (B).

Beneficial Ownership Directory	Central register of beneficial owners of companies and other legal entities.
Business relationship	A business, professional or commercial relationship between the client and the obliged entity which is connected with the professional activities of an obliged entity and which is expected by the obliged entity, at the time when the contact is established, to have an element of duration.
Client	A natural or legal person or legal arrangement which aims to enter into a business relationship or carry out an occasional transaction with an obliged entity in or from the Republic of Cyprus.
Compliance officer	Appointed individual, senior staff member of the firm with skills, experience and knowledge in AML/CFT compliance and overall financial activity, responsible for managing all aspects of the AML/CFT compliance program.
Economic Profile	Data and information regarding the client business activities, pattern and level of transactions and other relevant information. The Economic profile of the client is part of the Client Due Diligence.
EU Directive	Directive 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending regulation (EU) number 2012/648 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC.
FATF	The Financial Action Task Force. An inter-governmental body

	responsible to develop policies to combat money laundering.
Group	A group of undertakings which consists of a parent undertaking, its subsidiaries, and the entities in which the parent undertaking or its subsidiaries hold a participation, as well as undertakings linked to each other by a relationship within the meaning of Article 22 of Directive 2013/34/EU.
High risk third country	A third country, designated by the Commission pursuant to the provisions of Article 9 of the EU Directive by the issuance of acts by way of derogation, which presents strategical shortcomings in its national system for combating money laundering and terrorist financing which are considered as important threats for the financial system of the European Union, and a third country, which is categorised by the obliged entities as high risk in accordance with the risk assessment foreseen by section 58A of the Law.
ICPAC Directive	The present ICPAC Directive.
ICPAC members or members of ICPAC	All persons registered as members of ICPAC under the provisions of regulation 2.100 and 2.200 of the Members Handbook.
Illegal activities	The predicate offences mentioned in section 5 of the Law.
Information	Any form of written or oral information, data or documents including information which may be kept in a computer, in electronic form.
Laundering offences	The offences referred to in section 4 of the Law.
MOKAS	The Financial Intelligence Unit of the Republic, responsible for Combating Money Laundering and established under section 54 of the Law, also known as the Unit or the FIU.
Moneyval	The permanent monitoring body of the Council of Europe entrusted with the task of assessing compliance with the principal international standards to counter money laundering and the terrorist financing of terrorism and the effectiveness of their implementation.
National Risk Assessment Report (NRA)	A report, prepared to identify, assess and understand the country's money laundering and terrorist financing threats and vulnerabilities. It is an obligation for all EU members in accordance with Article 7 of the 4th EU AML/CFT Directive and pursuant to the Recommendations of the Financial Action Task Force.
Obliged entity	Any of the entities mentioned in section 2A of the Law, including all ICPAC members.
Occasional	Any transaction other than a transaction which is carried out during the

Transaction	normal duration of a business relationship.
Person	Any natural or legal person.
Politically Exposed Person (PEP)	A natural person who is or who has been entrusted with prominent public functions in the Republic or in another country, an immediate close relative of such person, as well as a person known to be a close associate of such person: Provided that, for the purpose of the present definition, 'prominent public function' means any of the following public functions: (a) heads of State, heads of government, ministers and deputy or assistant ministers, (b) members of Parliament or of similar legislative bodies, (c) members of governing bodies of political parties, (d) members of Supreme courts, of constitutional courts or of other high-level judicial bodies, the decisions of which are not subject to further appeal, except in exceptional circumstances, (e) members of courts of auditors or of the boards of central banks, (f) ambassadors charges d' affaires and high ranking officers in the armed forces, (g) members of the administrative, management or supervisory bodies of State-owned enterprises, (h) directors, deputy directors and members of the board or equivalent function of an international organisation, (i) Mayors No public function referred in points (a) to (i) shall be understood as covering middle-ranking or more junior officials. Close relatives of a politically exposed person includes the following: (a) The spouse, or a person considered to be equivalent to a spouse, of a PEP, (b) The children and their spouses, or persons considered to be equivalent to a spouse, of a PEP, (c) The parents of a PEP, 'Persons known to be close associates of a politically exposed person' means a natural person who: (a) Is known to have joint beneficial ownership of legal entities or legal arrangements, or any other close business relations, with a politically exposed person, or (b) Has sole beneficial ownership of a legal entity or legal arrangement which is known to have been set up for the de facto benefit of a politically exposed person.
Predicate offences	Any offence which is defined as a criminal offence by any law of the Republic.

Prescribed offences	Laundering offences and Predicate offences.
Property	Assets of any kind, whether corporeal or incorporeal, movable assets including cash, immovable assets, tangible or intangible, and legal documents or instruments in any form including electronic or digital, evidencing title to or an interest in such asset.
Republic	The Republic of Cyprus.
Risk Appetite	The amount and type of risk that an organisation is willing to take in order to meet its strategic objectives. Firms may have different risk appetites depending on the services they provide, their resources, culture and objectives. Risk appetite may change over time.
Risk Assessment	A process of evaluating the potential money laundering and terrorist financing risks that may be involved in a client business relationship.
Senior Management	Officers or employees of an obliged entity, being members of the Board of Directors for Companies, Partners for partnerships, Sole traders and other position in a different type of entity or legal arrangement, with top decision-making authority.
Senior Management Official (SMO)	An officer or employee of an obliged entity with sufficient knowledge of the obliged entity's money laundering and terrorist financing risk exposure and sufficient seniority to take decisions affecting its risk exposure. The 'senior management official' does not have to be a member of the Board of Directors of the obliged entity.
Supervisory Authorities	The Competent Supervisory Authorities mentioned in section 59 (1) of the Law.
Suspicion	The act or an instance of suspecting something wrong without proof or evidence. It is based on some information but the person making the suspicion report does not have to be 100% certain that Money Laundering or Terrorist financing has occurred.
Terrorist financing	The provision or gathering of funds by any means, directly or indirectly, with the intention to use such funds or knowing that they will be used in whole or in part for the commission of an offence within the meaning given to the term by section 4 of the International Convention for the Suppression of the Financing of Terrorism (Ratification and Other Provisions) Law and by sections 5 to 13 of the Combating of Terrorism Law.
The Institute or ICPAC	The Council of the Institute of Certified Public Accountants of Cyprus. ICPAC is the Supervisory Authority for its members under the Law.
The Law	The Prevention and Suppression of Money Laundering and Terrorist

	Financing law of 2007 L188(I)/2007 as amended in 2010, 2012, 2013, 2014, 2016 and 2018 by Laws 58(I)/2010, 80(I)/2012, 192(I)/2012, 101(I)/2013, 184(I)/2014, 18(I)/2016, 13(I)/2018 and 158(I)/2018.
Third country	A country not member of the European Union or contracting party to the agreement of the European Economic Area signed in Porto on the 2nd of May 1992 and adjusted with the Protocol signed in Brussels on 17 May 1993, as amended.
Trust	A written legal arrangement with which the settlor transfers property to one or more trustees who hold it for the benefit of one or more persons/beneficiaries.
Trust and Company Service Providers	Any person whose business is regulated and provides any administrative services as defined by article 4 of the "Law regulating companies providing administrative services and related matters of 2012" and further amendments.

It is noted that in this directive words importing the masculine gender include the feminine gender as well.

1.1.2 The word "**firm**" is used throughout to include sole practitioner, partnership and limited liability company involved in the provision of audit, external accounting, tax advisory, insolvent services, trust and company administration services. It is noted that insolvency practitioners obtain their license only as natural persons, yet for the purpose of this Directive we will be referring to them as firms.

1.2 Introduction

1.2.1 The main purpose of **the Law**, is to define and criminalise the actions involving the use and concealment of proceeds generated from predicate offences, laundering offences and terrorist financing activities. The Law provides amongst others for the confiscation of such proceeds aiming at depriving criminals from the profits of their crimes. This Directive, aims to outline the obligations of ICPAC members under the provisions of the Law.

1.2.2 The Institute is the **competent Supervisory Authority** responsible to monitor its members pursuant to the Prevention and Suppression of Money Laundering Activities Law of 2007 – 2018. In May 2015, the European Parliament and the Council adopted Directive 2015/849 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing. Cyprus has harmonised its legislation with the EU Directive during 2018.

1.2.3 **Firms** have a legal obligation to follow best practices for the prevention and suppression of Money Laundering and Terrorist Financing, to avoid having their services being abused by criminals, involved in money laundering or terrorist financing. Accountants, Auditors, Tax advisors, Insolvency practitioners, Trust and Company Service providers and other professionals are frequently referred to as **gatekeepers** in a number of typologies, risk damaging their reputation and business if they become involved in any way with money launderers or terrorist financiers, even unintentionally.

1.2.4 Firms may provide a wide range of services. **Services** falling under the scope of the Law may include the following:

i. Audit and assurance services
ii. Book-keeping and the preparation of annual and periodic accounts
iii. Tax compliance work
iv. Tax advice
v. Trust and company services as defined in article 4 of the Law Regulating Companies Providing Administrative Services and Related Matters
vi. Internal audit (as a professional service), and advice on internal control and risk management
vii. Insolvency/receiver-managers/bankruptcy related services
viii. Advice on structuring of transactions
ix. Forensic accounting

1.3 Scope of this Directive

1.3.1 ICPAC Directive has been prepared to give a **practical interpretation** of the Law so as to assist firms to comply with the provisions of the Law and assist the Supervisory Authority in determining whether a firm has complied with the requirements of the Law. The present Directive is binding and obligatory as to its adoption by the persons to whom it is addressed. It specifies the way of applying the provisions of the Law, ensuring all ICPAC members have a solid point of reference for the implementation of effective measures for the prevention and suppression of Money Laundering and Terrorist Financing. Prevention and suppression of Money Laundering and Terrorist Financing is also frequently referred as Anti-Money Laundering (AML) and Counter Terrorist Financing (CTF) in this directive.

1.3.2 Obliged entities must adopt **best practices** in their internal controls, policies and procedures and take measures to prevent money laundering and terrorist financing as set out in Part VIII of the Law. Implementation of such measures is fundamental to avoid committing the money laundering offences summarised in section 1.5.1 of this Directive.

1.3.3 The Law requires that all firms apply adequate and **appropriate policies**, controls and procedures, in order to mitigate and manage the risks as well as prevent money laundering and terrorist financing effectively, in relation to the following:

(a) Client identification and Client Due Diligence (CDD)
(b) Record-keeping

(c) Internal reporting and reporting to MOKAS
(d) Internal control, risk assessment and risk management
(e) Examination of transactions which by their nature may be considered vulnerable for money laundering or terrorist financing including complex or unusual large transactions and patterns of transactions with no clear economic benefit, commercial rationale or lawful purpose
(f) Making employees aware of the internal systems and procedures in relation to (a) to (e) above, the Law, the ICPAC Directive, the EU Directives and the relevant requirements for personal data protection
(g) Training employees in the recognition and handling of transactions and activities which may relate to money laundering or terrorist financing
(h) Recruitment and assessment of employees' integrity
(i) Risk assessment practices
(j) Compliance management

Appropriate controls and procedures established by firms in the areas mentioned above, should be proportional to the nature and size of the firms.

1.3.4 There are practical benefits in applying standard practices by all firms and across their entire range of services. **Consistency** of approach ensures complete coverage of the areas mandated by the Law and avoids difficulties with clients and persons who receive or provide services. For example, standard procedures to require senior management and staff to report any suspicion of money laundering or terrorist financing in the course of their work not only ensure that the requirements of the Law are met whenever they apply, but also give protection to individuals against breaching the disclosure provisions of primary legislation.

1.4 What is money laundering

1.4.1 **Money laundering** is any act or attempted act to conceal or disguise the identity of illegally obtained proceeds so that they appear to have originated from legitimate sources.

It usually involves three stages:

A. **Placement** – Placement of illicit funds in the financial system.
B. **Layering** – The actions of distancing illegally obtained proceeds from their source via the creation of multiple and complex levels of financial transactions designed to disguise the audit trail and to provide anonymity.
C. **Integration** – Re-entrance of the illicit funds in the financial system appearing to be legitimate proceeds.

1.5 Money Laundering offences, penalties and defences

1.5.1 The Law outlines the **Laundering offences**, for any person who **(a) knows** or **(b) ought to have known**, that any kind of property constitutes proceeds from the commission of illegal activities and carries out any of the activities listed below:

i. Converts or transfers or removes such property,
ii. Acquires, possesses or uses such property,
iii. Conceals or disguises any relevant information to such property,
iv. Assists another person to convert or transfer or remove such property or evade the legal consequences of his actions,
v. Participates in, co-operates, conspires to commit, or attempts to commit and provides counselling or advice for the commission of any of the offences referred to above,
vi. Discloses information in relation to investigations carried out for laundering offences, to suspects or others, distorting the investigation process. Commonly known as **"Tipping off"**.

Knowledge is not defined in the Law but it may also include situations such as:

- Shutting one's mind to the obvious
- Deliberately refraining from making enquiries the results of which one might not care to have
- Knowledge of circumstances which would indicate the facts to an honest and reasonable person.

1.5.2 The above offences (i) to (vi) are **punishable** by 14 years imprisonment and/or a penalty of up to €500,000 where a person 'knows' of a money laundering offence (case (a) of 1.5.1) and by 5 years imprisonment and/or a penalty of up to €50,000 where a person 'ought to have known' (case (b) of 1.5.1).

For the purposes of money laundering and/or terrorist financing offences:

- It is not significant whether the predicate offence is subject to the jurisdiction of the Cyprus Courts or not,
- There is no requirement for a prior or simultaneous conviction of a predicate offence, from which proceeds were derived,
- There is no requirement to prove the identity of the person who committed the predicate offence from which proceeds were derived.

It must also be highlighted that firms would not be expected to know the exact nature of the criminal activity concerned, or that particular assets are definitely those arising from the crime.

1.5.3 Further to "**Tipping off**" outlined in 1.5.1 (vi) above, no person should disclose any information to the client or a third person which may cause obstruction or negatively interfere with interrogations and investigations carried out. This includes information relating to suspicious transactions that has been or will be transmitted to MOKAS.

A case where a member of ICPAC during his professional activities, attempts to prevent a client from getting involved in illegal activities, is not considered as disclosure of information within the meaning of the present section.

The prohibition on disclosure of information ("Tipping off provisions") mentioned above does not prevent the disclosure between persons who carry out professional auditing activities, or external accounting activities, tax advisors, trust and company service providers and independent legal counsellors from third countries, as long as they impose requirements equivalent to those imposed by the EU Directive, and which carry out their professional activities, under any form of cooperation or engagement within the wider structure to which the person belongs and which share common ownership, management or compliance control.

In cases which relate to the same client and the same transaction, involving two or more obliged entities carrying out professional auditing activities, or external accounting activities, tax advisors, trust and company service providers and independent legal counsellors, the disclosure of information does not constitute an infringement of the law nor a breach of any contract, provided that the relevant obliged entities are from an EU member state or entities in a third country which imposes requirements equivalent to those laid down in the EU Directive. Additionally, they must all belong to the same professional category and be subject to obligations as regards professional secrecy and personal data protection.

The Tipping off provisions do not apply in relation to disclosure of information to Supervisory Authorities, including ICPAC, or disclosures for law enforcement purposes.

Any person who breaches the "Tipping off provisions" commits a criminal offence and may be subject to imprisonment of 2 years and/or a fine of €50.000.

1.5.4 In criminal proceedings against a person in respect of assisting another person to commit a money laundering offence or terrorist financing, it is in his **defence** if he intended to disclose to MOKAS his suspicion about the concerned activity or transaction and his failure to make the disclosure was based on reasonable grounds. It must be highlighted that any such disclosure should not be treated as a breach of any restriction upon the disclosure of information imposed by any contract. In case of employees of obliged entities, the Law recognises that the disclosure may be made to the Compliance Officer in accordance with established internal procedures and such disclosure shall have the same effect as a disclosure made to MOKAS.

1.5.5 Any person, including ICPAC members, who in the course of his trade, profession, business or employment, acquires knowledge or reasonable suspicion that another person is engaged in money laundering or financing of terrorism must disclose the said information to MOKAS. If this information is not disclosed, as soon as it is reasonably practical after the information came to his attention, then this is considered an offence. **Failure to report**, is punishable on conviction by a maximum 2 years imprisonment and/or a fine not exceeding €5,000.

1.5.6 ICPAC may impose and publish **administrative fines** for failure to comply with any of the requirements of the Law, to an ICPAC member of up to €1,000,000. In case the offenders' benefit from the breach exceeds €1,000,000, the administrative fine may increase up to twice the amount of the derived benefit. Where the offence continues, an additional administrative fine of up to €1,000 is imposed for every day that the offence continues.

Furthermore, an ICPAC member who fails to comply with the requirements of the Law may be referred to the Disciplinary Committee of the Institute for disciplinary action. The disciplinary action may result to an amendment or suspension or withdrawal of the member's license and/or a temporary ban. This is irrespective of whether money laundering or terrorist financing has taken place.

1.6 Members employed outside practice

1.6.1 While this Directive has been prepared primarily for ICPAC practicing members, much of the material, will also apply to members of the Institute employed elsewhere. **Members of ICPAC employed in other sectors** of the economy, may also find a more relevant directive prepared by their respective supervisory authority. In the absence of a relevant directive, members should consider the procedures recommended for ICPAC members in this Directive, and adopt them for their own circumstances as appropriate.

1.7 Vulnerability of firms to money laundering and terrorist financing

1.7.1 ICPAC members, are **vulnerable** to money launderers and terrorist financiers due to the fact that the specialised services they provide and the expertise they have in various practices may be used by money launderers and terrorist financiers to provide cover to their illegal activities. The quality of operations and AML policies in each firm, including the commitment from senior management, plays a crucial role in protecting the financial system as a whole. It is therefore of fundamental importance for a firm, to adopt a strong AML

Compliance culture approach, minimising the risk of exposure and abuse of its functions by money launderers and terrorist financiers. Hence, a member of the Senior Management shall be designated to have the responsibility for the implementation of the Law.

1.8 Responsibilities of the Institute

1.8.1 The Institute has an obligation to **monitor, evaluate and supervise** the application of the Law implementing a risk based approach to supervision using onsite and offsite reviews for ICPAC Members. This is achieved via the AML/Rules and Regulations monitoring tool which is outsourced to the Association of Chartered Certified Accountants (ACCA). See circular 12/2015.

1.8.2 In the context of supervision, ICPAC may request any of its members that failed to comply with the provisions of the Law or the present Directive, to take certain **measures** within a specified time frame in order to resolve the situation.

1.8.3 Furthermore, all supervisory authorities, including ICPAC, may impose Administrative fines as per paragraph 1.5.6 above. ICPAC may decide not to publish any administrative fines on the grounds of a) Disproportionality, b) Jeopardy of the stability of the financial markets or c) Jeopardy of an ongoing investigation. In case an administrative fine is published, it must remain for 5 years on ICPAC website and should be in full alignment with Processing of **Personal Data** (Protection of the Individual) Law.

1.8.4 The Institute also encourages **reporting of potential or actual breaches** of ICPAC Members in relation to the Law, simultaneously ensuring protection of all affected natural persons in accordance with the provisions and principles of the Processing of Personal Data (Protection of the Individual) Law. Such breaches can be reported online though filing an electronic complaint form.

1.8.5 ICPAC has specific obligations under the Law to report to the Attorney General and MOKAS any information it obtains which is or may be, relevant to money laundering or terrorist financing. Based on this obligation, the Institute may ask and collect information from firms and **exchange this information** with MOKAS and other Supervisory Authorities.

1.8.6 **Statistical data** on matters relating to their competences must be collected and maintained by all competent Supervisory Authorities, including ICPAC. These statistical data may be transmitted to the EU Commission, used in the National Risk Assessment and the Evaluation of the Council of Europe's "Moneyval" Commission.

1.9 Court orders for disclosure of information

1.9.1 Courts in Cyprus may, on application by the investigator, make an order for the disclosure of information by a person, including a firm, who appears to the Court to be in possession of the information to which the application relates. Such an order applies irrespective of any legal or other provision which creates an obligation for the maintenance of secrecy, confidentiality or imposes any constraints on the disclosure of information. The obligation for disclosure remains for any subsequent change in the information and/or any subsequent information which relates to the subject matter of the **court order for disclosure**. As already stated under “tipping off provisions”, a person who makes any disclosure which is likely to obstruct or prejudice an investigation, knowing or suspecting that the investigation is taking place, is guilty of an offence.

1.9.2 A third party claiming to be entitled to assets which are or have been in the hands of a firm and which are the subject of a report to MOKAS, might also seek a **court order** which would direct the firm to disclose information. If the firm believes that disclosure of information to the **third party** could prejudice a money laundering or terrorist financing investigation by the law enforcement agencies, the tipping off offence could arise. Legal advice should be obtained before the information is disclosed.

2 Internal Controls, Policies and Procedures

2.1 Responsibilities and accountabilities

2.1.1 Firms are required to establish and maintain **policies, procedures and controls** proportional to their nature and size, so as to mitigate and manage the risks as well as preventing money laundering or terrorist financing, ensuring the reporting of any transactions or activities that may be known or suspected.

2.1.2 More specifically, obliged entities should have in place **appropriate procedures** in relation to the following:

(a) Appointment of a Compliance Officer (Chapter 3)
(b) Adoption of Risk Assessment and Risk Management policies for AML & CTF (Chapter 4)
(c) Client Identification and Due Diligence (Chapter 5)
(d) Record keeping and data protection (Chapter 6)
(e) Ongoing monitoring (Chapter 7)
(f) Recognition and reporting of Suspicious Transaction & Activity Reports (STRs & SARs) (Chapter 8)
(g) Training and Awareness of staff members (Chapter 9)

2.1.3 All firms should document the procedures implemented and the controls applied in relation to (a) - (g) above in a **manual**, to prevent money laundering and terrorist financing. The manual and procedures adopted must be approved by Senior Management officials of the firm. Arrangements should also be made to update the manual in accordance with the latest provisions of the Law and the risk appetite of the management.

2.1.4 Firms should make arrangements to verify, on a regular basis, the compliance with and the **effectiveness** of policies, procedures and controls. Firms may consider obtaining assurance from independent professionals.

Where appropriate and proportional to the size and nature of their activities, an independent internal audit service covering the AML/CFT system of the firm, should be established for **verification** of internal policies, controls and procedures.

2.1.5 Firms should designate a member of the **Board of Directors or senior partners**, provided there is a Board, which shall be responsible for the implementation of the procedures outlined in 2.1.2 above.

It is noted that in cases where a natural person which is an ICPAC member and falls under the definition of obliged entities/persons and practices the profession as an employee of a legal person which is also an obliged entity, then obligations deriving from the Law relating to internal procedures, training and feedback, apply to that legal person rather than to the natural person.

2.1.6 Firms should take necessary measures to assess their **employee's integrity** not only on recruitment but also on an ongoing basis.

2.2 Overseas offices and associated firms

2.2.1 Firms may belong to a group, implementing **group-wide policies** and procedures for AML and CTF purposes, including procedures for sharing information. In such cases, the firm should ensure that these group-wide policies and procedures are applied effectively throughout the group and are at least as strict and as effective as the provisions of the Law and the present directive for due diligence and identification purposes and the corresponding data protection requirements.

2.2.2 In cases of firms belonging to **groups operating in third countries** where the laws of the said third countries do not permit the application of the above outlined policies and procedures, then the member of ICPAC must inform ICPAC and take additional measures to mitigate the increased risk of money laundering and terrorist financing.

3 Compliance Officer

3.1 Appointment of the Compliance Officer

3.1.1 All firms should **appoint** a **Compliance Officer (CO)**. The person appointed as CO should be sufficiently senior employee, with sufficient skills, experience and knowledge in AML/CTF and Compliance areas as well as knowledge of the firm, its service lines and its clients. The CO must also have the necessary authority to fulfil his duties which may include taking decisions affecting the risk exposure of the firm and the handling of Internal and External STRs and communication with MOKAS and the Institute.

3.1.2 In cases where the CO is not a member of the Board of Directors, a member of the **Board of Directors** should be **designated** to be responsible for the implementation of the Compliance policies and procedures in accordance with the Law.

3.1.3 Firms should **communicate to MOKAS** the name and position of the person whom they appoint to act as Compliance Officer.

3.1.4 Firms must ensure that the CO has sufficient resources to undertake the work associated with the role. Depending on the size, complexity and structure of an obliged entity, the firm may appoint Chief and assistants. The **role and responsibilities** of the CO including those of Chief and Assistants should be clearly specified by the firm and documented in appropriate manuals and/or job descriptions. The CO should be allowed direct and timely access to all documents, data and information possessed by the firm which may assist him in carrying out his duties. COs should undertake annually at least 10 Continuous Professional Development (CPD) units, specialised and relevant to their Compliance functions, in accordance with section 2.700 paragraph 4(9) of the ICPAC Members handbook.

3.2 Role of the Compliance Officer

3.2.1 The role of the **Compliance Officer** is not defined in the Law but has traditionally included responsibility for internal controls and risk management around money laundering and terrorist financing subjects, in accordance with guidance issued by the regulator. More specifically, the CO as a minimum should:

(a) Provide for the design and implementation of the systems and controls needed to enable staff to make internal suspicious reports. Must also ensure that the reporting lines are clear and communicated to everyone.

(b) Receive from the firm's employees any information or other matter that creates suspicions of Money Laundering and Terrorist Financing (STRs & SARs). See Chapter 9.

(c) Examine and validate the information received as per paragraph (b) above by reference to any other relevant information, discuss the circumstances of the case with the reporting employee and where appropriate, with the employee's superior(s). The evaluation of the information reported, and the examination performed should be recorded and retained. See chapter 6 for more details on record keeping.

(d) Following (c) above, the CO may decide to notify MOKAS. He should then use the GoAML website to complete a Suspicious Transaction Report (STR) or a Suspicious Activity Report (SAR) and submit it to MOKAS the soonest possible. See Chapter 9 for more information.

(e) Act as the first point of contact with MOKAS, upon commencement of and during investigation as a result of filing an STR or SAR to the MOKAS under (d) above. The CO also provides all the supplementary information requested and ensures full cooperation with MOKAS.

(f) Create, maintain and be involved in the firms' risk based approach for the prevention of Money Laundering and Terrorist Financing including the client risk assessment process, taking into consideration the findings of the National and Supranational Risk Assessment.

(g) Develop Client Due Diligence (CDD) policies and procedures.

(h) Provide support, advice and guidance to management and other employees of the firm on money laundering and terrorist financing matters and determine whether the firm's employees need further training, awareness and knowledge for the purpose of combating money laundering or terrorist financing.

(i) Remain up to date with best practices, recent trends, ICPAC circulars and technical alerts including the use of national and international findings like the various National and Supranational Risk Assessments, the EU Commission, FATF, Moneyval, the Egmont group, the Basel committee, the IMF, Transparency International and other to improve the firm's internal procedures for recognising and reporting money-laundering and terrorist financing suspicions

(j) The Compliance Officer is primarily responsible, in consultation with the firm's senior management and Internal Audit Department (if applicable), towards the Institute in implementing the various Directives issued by ICPAC under the Law as well as all other instructions/recommendations/circulars issued by the Institute, from time to time, on the prevention of the criminal use of services offered by firms for the purpose of money laundering or terrorist financing. The CO must also prepare and submit to the Institute the Annual Compliance Officer report and the AML Questionnaire annually in accordance with ICPAC guidelines updated from time to time.

(k) Depending on the size and activities of the obliged entity, a CO may consider preparing a report to the Board of Directors (or equivalent managing body) at least annually, giving an assessment of the operations and effectiveness of the firms' AML systems and controls. This should take the form of a written report. These written reports should be supplemented with regular ad hoc meetings or comprehensive management information to keep senior management engaged with AML compliance and up-to-date with relevant national and international developments in AML, including new areas of risk and regulatory practice. The board (or equivalent managing body) should be able to demonstrate that it has given proper consideration to the reports and ad hoc briefings provided by the CO and then take appropriate action to remedy any AML deficiencies highlighted.

3.2.2 The Compliance Officer is expected to make every reasonable effort to mitigate the risk of **errors and/or omissions** in the course of discharging his duties and, most importantly, when validating the reports received on money laundering or terrorist financing suspicions, as a result of which a report to MOKAS may or may not be submitted.

3.2.3 He is also expected to **act honestly and** reasonably and to make his determination **in good faith**. It should be emphasised that the CO's decisions may be subject to the subsequent review of the Institute. ICPAC, in the course of examining and evaluating the procedures of a firm against money laundering or terrorist financing, and their compliance with the provisions of the Law, is legally empowered to report to MOKAS a firm and/or a client of a firm which, in its opinion, does not comply with the provisions of the Law and forms the opinion that actual money laundering or terrorist financing has been carried out.

4. Risk Based Approach (RBA)

4.1 How to use RBA

4.1.1 The application of risk based approach is fundamental to comply with **the Law**, the EU directive and the FATF recommendations. It forms the foundations on which the firms' AML policies, controls and procedures, and more importantly its CDD and staff training procedures should be based on. Therefore, it is of paramount importance for a holistic and dynamic risk-based approach to be used.

4.1.2 The **risk-based approach** also identifies the money laundering and terrorist financing risks posed by each client and provides for a unique assessment of every client relationship, allowing firms to tailor their actions in proportion to their risk appetite. Each firms risk appetite may vary, according to the objectives of the senior management.

RBA allows firms to exercise reasonable business and professional judgement and scepticism with respect to clients regarding the management of potential money laundering and terrorist financing risks. It allows firms to allocate resources and efforts where the identified risk is greatest and conversely, reduce requirements where the identified risk is low. It also allows firms to adjust and adapt in a more effective and efficient manner, as new money laundering and terrorist financing methods are identified.

4.1.3 It must be noted that **RBA** does not exempt low risk clients from **CDD**, nonetheless, the appropriate level of CDD is likely to be less onerous than for higher risk clients. In all cases ongoing monitoring procedures must always be carried out. See chapter 5 for more details.

4.1.4 RBA has a number of **positive characteristics**, namely:

a) It gives a better **insight** – It recognises that the money laundering or terrorist financing threat varies across clients, countries, services and financial instruments,
b) It is **flexible** – It allows firms to differentiate between clients in a way that matches the risk of their particular business,
c) It provides for the firms' **Risk Appetite** – It allows firms to apply their own approach in the formulation of policies, procedures and controls in response to the firm's particular circumstances and characteristics,
d) It is **efficient** and **effective** – It helps to produce a more cost effective system, and
e) It is **proportionate** – It promotes the prioritisation of efforts and actions of the firm in response to the probability of money laundering or terrorist financing occurring through the use of services provided.

4.1.5 In the implementation **of a RBA**, for assessing the most cost effective and proportionate way to manage the money laundering and terrorist financing risks posed by clients, a firm ~~may~~ must follow the below ~~indicative~~ **steps**:

a) Determining the risk appetite of the firm, to be decided at senior management level and which should be reflected ~~documented~~ in the Client Acceptance Policy,
b) Identifying and assessing the money laundering and terrorist financing risks emanating from particular clients, services, geographical areas of operation of the

firm and its clients and service delivery channels

c) Managing and mitigating the assessed risks by the application of appropriate and effective measures, procedures and controls,
d) Continuous monitoring and improvements in the effective operation of the policies, procedures and controls,
e) Design and document ~~Documenting~~ the procedures and controls in appropriate manuals and policies, to ensure uniform application across the firm.

More details can be found on RBA best practices guidelines published by ICPAC in GC_6/19 on 11 March 2019.

4.2 Tone at the top

4.2.1 Each firm's senior management officials should establish the acceptable risk profiles of its clients. These should be documented in a **Client Acceptance Policy (CAP)**, which will also outline the characteristics of a potential client, that the firm should potentially decline the application for establishment of a business relationship. For example, business relationships with PEPs from high risk countries, depending on the risk appetite of the firm.

In the Client Acceptance Policy, senior management officials should outline the client acceptance criteria on which the RBA implementation and Economic profile of a client will be based on.

4.2.2 As per the provisions of the Law, senior management should appoint a member of the Board of Directors as a **responsible person** for the implementation of the firms compliance programme, policies, controls and procedures. The above is of particular importance in cases where the Compliance Officer is not a member of the Board of Directors. Firms should also ensure that their compliance department has enough resources in human capital, trainings and technology, always proportional to the risk appetite, complexity and broadness of tasks to be undertaken.

4.2.3 Senior management must demonstrate commitment to compliance and the implementation of RBA, via their **involvement** in the Risk Assessment process of their clients. **Senior management officials** should also ensure that the CAP and corresponding risk management is refreshed regularly by periodic reviews, reflecting any significant changes that may take place in the business environment or the legal framework.

Senior management officials must also approve the policies, procedures and controls applied by their firms in relation to money laundering and terrorist financing, as well as monitor, and where appropriate, enhance the measures adopted.

4.3 Risk Categories

4.3.1 According to the Law and various typologies on RBA, money laundering and terrorist financing risks should take into account as a minimum, the following **risk factors**:

a) Country/Geographical risk
b) Service risk
c) Client risk
d) Delivery channels risk

In practice, these risks may overlap and should be viewed as inter-related. There is no single methodology to apply to these risk categories, and their application is merely intended to provide a suggested framework for approaching the management of potential risks.

4.3.2 When implementing a RBA the assessment of risks may change according to time and global developments, therefore it must be highlighted that this is a dynamic process and must be maintained. A static implementation of the RBA may lead to a distorted picture and complicated circumstances, increasing the business risks of each firm. Firms may refer to Annex I for low risk indications, Annex II for high risk indications and the RBA guidelines of ICPAC for examples on the **implementation of RBA**. The examples provided are given for assistance in identifying those that may apply in the circumstances of individual firms and client relationships. However, it should be borne in mind that the lists of examples provided are not exhaustive.

Firms should make use of reliable publicly available information when attempting to evaluate the risk of their clients. Some of the reliable sources include the following:

(a) The latest Supranational Risk Assessment of the EU commission
(b) The National Risk Assessment of Cyprus including other reliable governmental sources or circulars
(c) ICPAC circulars and announcements on the subject
(d) MOKAS circulars and announcements on the subject
(e) Other reputable sources mentioned in section 4.5.3

As mentioned above, the core of RBA includes the assessment of risk of a firm's clients, geographical locations, the services provided and the transactions or delivery channels. Summarised below are the main risk factors that can be used for the Client Risk Assessment (CRA).

Country/Geographical risk

4.3.3 There are various elements to consider when assessing geographic risk. Some examples include the perceived level of fraud, bribery and corruption, funding terrorism, criminal activity, and the effectiveness of money laundering and terrorist financing legislation and controls within the country or geographical area. Additionally, country sanction regimes or embargoes imposed by the EU and the UN should also be taken into consideration.

Some geographical areas or countries may be perceived to have a higher risk level, yet clients with extensive experience in a certain geographical area or country may bare a different geographical risk level than a client with limited experience. Nevertheless, clients may be judged to pose a higher than normal risk where themselves, their associates, BOs, operations or their source or destination of funds, are located in a country that poses a higher risk (see Annex II).

Service risk

4.3.4 A risk assessment should determine the potential risk presented by the services offered by a firm to a client. Firms should consider carrying out additional checks when providing a service that has an increased level of money laundering and terrorist financing vulnerability concerning the offences outlined in section 1.5.1. Some types of services may be of particular interest to money launderers and terrorist financiers, due to their nature, and therefore carry a higher degree of risk (see Annex II).

Provision of services relating to the naturalisation of or the acquisition of citizenship through the Cyprus Investment Programme, are to be treated as high risk by default.

Abuse of services provided by ICPAC members may lead to amongst others to the following negative outcomes:

- Misuse of introductory services, e.g. to financial institutions leading as a minimum to reputational damage
- Misuse of pooled client accounts or safe custody of client money or assets
- Advice on the setting up of legal arrangements, which may be used to obscure ownership or real economic purpose (including setting up of trusts, other complex group structures, companies or changes of name/corporate seat).

The above list is non exhaustive and more information on service risk can be found in the RBA guidelines of ICPAC.

4.3.5 In cases where a firm will start providing a **new service** which is significantly different from its existing range of services, it should assess the corresponding money laundering and terrorist financings risks. According to the results of the assessment performed, the firm should act proportionally.

Client risk

4.3.6 Outlined below are the key indicators associated with increased client risk factors:

a. Indications that the client is attempting to hide information on the operations of its business, ownership or nature of its transactions
b. Indications that certain transactions, structures, geographical locations, international activities and other are not aligned with the firm's understanding of the client's business or economic profile
c. Client industries, sectors or categories where opportunities for money laundering or terrorist financing are particularly widespread
d. Secrecy and unnecessarily complex ownership structures that disguise ownership and control
e. PEPs involvement in the affairs of the client. See section 4.4 for more details.
f. Embargoes, sectoral sanctions, sanctioned designated nationals (SDNs), territorial or country sanctions. See section 4.5 for more details.
g. Clients that have applied for citizenship through the Cyprus Investment Programme.

The above list is non exhaustive and more information on client risk can be found in Annex I and Annex II as well as the RBA guidelines of ICPAC.

Delivery channels risk

4.3.7 Delivery channels of the provided services influence the money laundering and terrorist financing risk. The identity and credibility of a client may be more difficult to assess depending on the means of providing the services. More specifically, where clients have not been met face to face, or there is an involvement of a third party authorised to represent the client, the delivery channel risk is higher. The same approach should also be taken to business relationships with family members and associates of PEPs.

Firms should take into consideration the risks posed by a given delivery channel when performing their Client Risk Assessment (CRA). Where higher risk levels are identified, firms should establish mitigating controls. For higher risk factors relating to delivery channels see Annex II.

4.4 Politically Exposed Persons (PEPs)

4.4.1 In cases where the BO of a client is a PEP or where a PEP exercises control over the client, firms should **by default** treat the client as **high risk** from a money laundering and terrorist financing perspective. All firms must ensure the above is clearly accounted for in their risk management policy. In such cases, Enhanced Due Diligence measures should apply. See section 5.7 for more details.

4.4.2 A **PEP** generally is perceived to present a higher risk for potential involvement in bribery and corruption by virtue of their position and the **influence** they may hold. This influence is also considered to have an effect on the risk profile of their close family members and associates. Close family members and associates of PEPs should also be treated as high risk.

4.5 Cyprus Investment Program (CIP)

Citizenship by Investment Schemes carry inherent risks related to money laundering, corruption and bribery, primarily due to the characteristics of the target group being addressed to, i.e., high net-worth individuals.

With a view to manage these risks, firms should apply mitigating measures.

New and existing clients requiring the provision of services to apply for a citizenship through the CIP should automatically be classified as high risk by default as a direct result of the provision of the specific service (*service risk*). In this case, the firm should determine the depth and extent of EDD measures to be applied. See section 5.7 for more details.

Following the attainment of the citizenship and in the event that the firm continues to maintain a business relationship with the client (through the provision of other services that fall within the scope of the AML/CFT Law), the firm should account for this in its risk assessment process and more specifically through allocating an element of higher *client risk*.

An element of higher *client risk* should also be allocated to clients for whom services related to the CIP have been provided by another professional or clients who have been denied citizenship through the CIP, but with whom the firm has a business relationship (through the provision of other services that fall within the scope of the AML/CFT Law). In the eventuality of refusal of the granting of citizenship, the reasons for the refusal must be documented and taken into consideration when implementing the risk-based approach.

It is highlighted that in cases where a client is of Cypriot nationality attained through the CIP, it is the origin of the client that should be taken into consideration when assessing the *country/geographical risk* during the risk assessment process and not the nationality of the client.

Firms are also expected to take reasonable steps to identify whether clients or potential clients participated to citizenship by investment programmes in other jurisdictions. In case where a client with the above characteristics is identified, the corresponding risk should be taken into consideration and mitigating controls must be applied.

4.6. Sanctions and Other factors to consider

4.6.1 During the implementation of RBA, careful consideration should be given to sanction related matters. More specifically, firms should ensure that they are in full compliance with a) EU restrictive measures (Restrictive Measures adopted by the Council of the EU via relevant Decisions and Regulations, within the framework of Common Foreign and Security Policy) and b) UN sanction programmes (International Sanctions by a relevant Decision/Resolution adopted by the Security Council (SC/UN), under chapter VII of the UN

Charter).

In case of non-compliance of an ICPAC member with the **EU restrictive measures and the UN sanction programmes**, the corresponding legislation provides for penalties of 2 years imprisonment and/or fine of €100,000 for individuals and €300,000 for legal entities. More information on the above can be found in the Ministry of Foreign Affairs website and the circulars issued by ICPAC on the subject.

4.6.2 Special attention must also be paid in other sanction regimes that may have an impact on the clients risk profile.

For example, **US sanctions** imposed by the Office of Foreign Assets Control (OFAC) do not need to be adhered to, according to the relevant legislation by obliged entities established in the Republic. Despite that, firms are encouraged to pay close attention to these sanctions and assess the risks emanating from any business relationships they may have with a sanctioned person. It must be highlighted that some US sanctions contain provisions for secondary sanctions. Secondary sanctions involve economic restrictions to non-US citizens and companies for doing business with a US sanctioned person [GC 7_2018].

4.6.3 Firms should design and implement **policies and procedures** enabling them to identify transactions which may be in violation of the EU Restrictive measures and the UN sanctions. The policies and procedures should be clearly documented.

4.6.4 Other high risk areas highlighted by **ICPAC circulars**, the National or Supranational Risk Assessments or typologies issued by other reputable international organisations like

- the EU Commission,
- FATF,
- Moneyval,
- the Egmont group,
- the Basel committee,
- the IMF,
- Transparency International

and **other** should be taken into consideration during the risk assessment design process. As noted above the implementation of RBA is a dynamic process which must be updated and maintained continuously.

ICPAC general circulars and technical alerts issued, cover areas like Cryptocurrencies and ICOs providing insight on subjects. All members are expected to follow the guidance provided as part of their compliance obligations.

4.7 Application of Risk based approach

4.7.1 For the **development of a RBA,** it is necessary for firms to review their internal affairs and consider what money laundering and terrorist financing risks might attach to each service type, client type etc. When performing the above mentioned exercise, the

proportionality principle should be taken into account.

Consideration of these risk types should enable firms to establish a qualitative risk assessment methodology. Firms may find it more convenient to draw up a simple scorecard of characteristics of the client or service which are considered to present a higher than normal risk, and those which present a normal risk. During this process firms must consider the risks factors outlined above. For example, long association and detailed knowledge of the client or listing on reputable stock exchanges may be considered as risk reducing factors. Refer to Annex I and II and the RBA guidelines of ICPAC for more details.

The qualitative risk assessment methodology or scorecard should reflect the provisions of the Client Acceptance Policy mentioned in section 4.2 above and must be one of the first steps of the client due diligence process. The process enables the firm to assign a money laundering or terrorist financing risk level to each client ensuring that the proportional client due diligence work is carried out. Enhanced due diligence measures should be carried out for those clients that are determined to be of higher risk. See chapter 5 for client due diligence provisions.

4.7.2 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 client due diligence that causes concern or suspicion.

4.7.3 In all cases, firms should gather information about the client ("know your client" also known as **KYC** which is part of the client due diligence process – see Chapter 5), to assist with the effective on-going monitoring and ensure understanding of the following:

- who the client is
- where applicable, who owns the client (chain of ownership up to and including beneficial owners)
- who controls the client
- the purpose and intended nature of the business relationship
- the nature of activities/business of the client (including detailed/thorough understanding of the client's activities and nature of transactions)
- the client's size and source of wealth and funds
- the client's business and economic purpose
- the client's group structure by also identifying any subsidiaries, associates or related companies with which the client transacts
- the commercial and business rationale behind the client's existence and whether it can be demonstrated that it exists for a legitimate trading or economic purpose

4.7.4 Firms need to set out clear **requirements** for collecting "**know your client**" information and for conducting verification of identity, to a depth suitable for the assessment of risk. As noted above, for clients that are classified as high risk, Enhanced Due Diligence (EDD) measures are required.

4.7.5 **EDD measures** and controls for higher risk clients and transactions may include:

a) Increased awareness across all departments with a business relationship with the client, including enhanced briefing of client teams.

b) Escalation of the approval process for the establishment or renewal of a business engagement, or involvement in the client service.

See section 5.7 for more details on EDD.

4.8. Documentation

4.7.1 Firms must be able to demonstrate to the Institute how they evaluate and mitigate money laundering and terrorist financing risks. The **risk based approach framework** adopted must be clearly **documented**, in line with the Client Acceptance Policy and made available to the Institute upon request.

4.7.2 All firms must document the **client risk assessment** performed for each individual client. The assessment must be in line with the principles outlined in the risk based approach framework and consistent across all client risk assessments.

5 Client Due Diligence (CDD)

5.1 Statutory requirements

5.1.1 Firms are required to maintain Client Due Diligence (CDD) procedures including identification and verification of clients, in accordance with the **provisions of the Law**. CDD is an integral part of a firm's AML policies. Its objective is to identify the client and comprehend the corresponding business activities, enabling the firms to understand, mitigate and manage the Money Laundering and Terrorist Financing risks. The KYC process is part of the CDD procedures.

Good knowledge of a client's business and financial background as well as information on the purpose and intended nature of the business relationship is also very important in order to provide an effective service, to the client.

5.1.2 It must be noted that before the establishment of a business relationship, commercial enquiries should be made to identify if the prospective client, has not been, or is not in the process of being **dissolved**, struck off, wound up or terminated. This is important for a firm to establish a better understanding of the real purpose of the business relationship.

Additionally, firms should be alert and corroborate accordingly, on the reasons why any of their existing and/or potential clients is changing professional service providers. Frequent and unjustifiable changes in professional service providers may be a red flag.

5.2 Identification, Verification of information and documentation received

5.2.1 The **basic principles** outlined in the Law regarding identification and CDD measures are the following:

(a) Identify and verify the **client** identity
(b) Identify and take reasonable steps to verify the **beneficial owner** identity and place of residence
(c) Take reasonable steps to understand the **ownership and control structure** of the client
(d) Take reasonable steps to assess the purpose of the intended nature of **business relationship**
(e) Conduct **ongoing monitoring** to confirm the information gathered initially

Firms should also identify and verify any 3rd persons having the mandate to represent the client and ensure that the said 3rd persons have a legitimate authority.

5.2.2 It is emphasised that firms should not rely exclusively on the central **register of beneficial owners** of companies and other legal entities (Beneficial Owner Directory) for the fulfilment of their CDD requirements, in accordance with the provisions of the Law.

5.2.3 Firms should conduct CDD in sufficient detail, so as to provide them with reasonable assurance and comfort, that the information they have obtained, depict an appropriate, satisfactory and sufficient indication of the true affairs of the client. The degree of detail and extend of procedures of **CDD** applied may vary according to the nature and purpose of activities, the ownership structure and the risk profile of the client. It is highlighted that the **Risk Based Approach** (see Chapter 4) should be taken into consideration in the proportional application of CDD.

5.3 When to carry out CDD

5.3.1 By Law firms must apply CDD measures **before** entering into a business relationship or carrying out an occasional transaction.

According to the legislation CDD should be completed when:

(a) **Establishing** a business relationship
(b) Carrying out an **occasional transaction** which is equal to or higher than **€15,000** irrespective of whether the transaction is carried out in a single operation or in several operations which appear to be linked
(c) There is a **suspicion** of money laundering or terrorist financing (regardless of the amount)
(d) There are **doubts about** the veracity or adequacy of **previously obtained CDD**

5.3.2 CDD procedures should be applied not only to all **new clients but also to existing clients** at appropriate times.

More specifically for existing clients, CDD procedures may be performed when the relevant circumstances of the client change or during scheduled/routine CDD updates.

Change-driven updates of the CDD may be triggered by

a) Suspicions,
b) Changes in the client BO,
c) Changes in services provided,
d) Changes in professionals servicing the client,
e) Changes in general affairs,
f) Changes in line of business,
g) Changes in geographical area of operations,
h) Changes in key management,
i) Application for or attainment of citizenship through the CIP, and
j) Any other changes.

Scheduled/routine CDD updates should be carried out on a risk sensitive basis. Hence the higher the risk the more frequent the scheduled CDD update should be carried out.

5.3.3 If a firm finds out, at any stage of the business relationship with an existing client, that valid or sufficient **documentation or information is not available** regarding his identity and economic profile, the firm must apply all necessary procedures and carry out due diligence measures in order to collect the missing documentation and information as quickly as possible, in order to form the complete economic profile of the client.

5.3.4 **Further enquiries** may be appropriate in cases where after the application of CDD procedures, the information and documentation obtained is not of sufficient quality to satisfy the firm that:

a) the identity of the prospective client and corresponding BO has been adequately verified or

b) there is a thorough understanding of the ownership and control structure or

c) there is enough information to assess the purpose and intended nature of business relationship.

If the firm, following further enquiries still has doubts or the client did not provide the information requested within a reasonable time, the business relationship may be declined or terminated. The firm should also examine the possibility of submitting a suspicious transaction report to MOKAS.

5.3.5 Firms are required to conduct background screening and perform background checks against sanctions lists and PEPs lists and in order to determine whether any negative information exists regarding the potential client that might affect the risk emanating from the client. Background screening should form part of the initial CDD process and during any change-driven updates of the CDD or during scheduled/ routine CDD updates. The results of the background screening should be appropriately documented and incorporated in the risk based process of the firm, e.g., high risk clients. Partial matches as well as false positives should be maintained with an explanation on why they do not pose a concern or why they have been disregarded as a match for further examination.

Depending on their size, nature and type of clientele, firms are encouraged to subscribe in a **specialist electronic database**. Firms using specialist databases should comprehend how these databases are populated and need to ensure that all findings from the database used are corroborated thoroughly before and during the client relationship. Special emphasis must be paid to high risk clients.

5.3.6 ~~5.3.5 If a firm suspects that a prospective client engages or intends to engage in money laundering or terrorist financing, it may well decline the business relationship but has a **legal obligation** to file a suspicious activity report to MOKAS. In that event it will be unnecessary to complete identification procedures.~~ The firm must terminate or refuse to enter into a business relationship – depending on the case – if it cannot comply with the identification, verification and evaluation of the nature of the business relationship requirements. The firm has also a **legal obligation** to examine the possibility of filing a suspicious report to MOKAS. Moreover, nothing must be communicated to the ~~prospective~~ client (or to any other person) which might prejudice an investigation or proposed investigation by the law enforcement agencies, as this will be considered as “tipping off”.

5.3.7 ~~5.3.6.~~ By way of derogation from the contents of the current section, a firm may allow the verification of the identity of the client and the beneficial owner to be completed **during the establishment of a business relationship,** if this is necessary for not interrupting the normal conduct of business and where the **risk** of money laundering or terrorist financing occurring is **low**. Such situations could include involvement of an ICPAC Member as a subject matter expert in appointments to ascertain the client's legal position or defend them in legal proceedings.

In such situations, these procedures shall be completed as soon as practicable after the initial contact.

5.4 Identification and verification of natural persons

5.4.1 The **identity** of a natural person comprises his name and all other names used, the date of birth and the address at which the person can be located. Additional information like his source and size of wealth, signature, his profession or occupation and any other relevant information should also be obtained if judged necessary to perform all obligations under the Law, always in accordance with the provision of the Processing of Personal Data (Protection of the Individual) Law.

5.4.2 As a general note, it is recommended that clients are met **face to face** whenever possible. Where not possible, mitigating steps (like for example video calling or future face to face meeting) should be taken to reduce the AML and CTF risk involved. In cases of video calls, the calls should be recorded and documented accordingly, and be readily available to MOKAS or ICPAC. A video call should not be considered equivalent to a face to face meeting, rather it is a means to establish direct communication with the client. It is highlighted that in cases of legal persons, the meetings should be held with the BO or the person who has the responsibility of the decisions and the management of operations of the client.

5.4.3 The identity and the place of residence of a natural person should be verified. Verification may require for example physical review of an original document (with a photocopy taken). It involves validating (with an independent, authoritative source), that the information gathered is accurate.

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 or place of residence is being verified. Documents issued or made available by an official body can be regarded as being independent.

Refer to Annex III for a non-exhaustive list of documents that can be used for verification purposes. Each firm may define the documents to be accepted for verification depending on its operations and risk appetite, without jeopardising a violation of the provisions of the Law.

5.4.4 Firms should be able to prove the source of the documentation gathered for verification purposes. In cases where the original document is seen by an employee of an ICPAC licensed firm, it should be sufficient for that person to copy the document and certify it as true copy of the original, including the date on which it was seen, as well as the name and capacity of the person **certifying** the document, as part of their internal KYC process.

In cases where the copy of the document verifying client information originates from third parties, all provisions of section 5.9 must be taken into consideration. Care must be taken to assess the risks associated with certified copies obtained from third parties (for example, documents may be forged).

5.4.5 The internet is also a very good source of information to reconfirm our understanding obtained during the CDD process. Publicly available information sources like website of a regulator, stock exchange, government department, company registers and land registries may also provide a useful insight, complementing the CDD policies outlined above. Firms though must be aware that the quality of such sources should be thoroughly assessed. For example, sources which allow users to amend the content at will, should never be used.

Where such documents are used, they should be annotated. By **annotation** it is meant to clearly indicate the source (web address which was printed from), the date (when the printing/download took place) and the name and signature of the person who performed the print/download.

5.4.6 In the event where ~~any person~~ a client or any person representing the client or a third person upon which reliance has been placed for that client, during the performance of the procedures for client identification and due diligence measures, knowingly provides false or forged or misleading evidence or information for the identity of the client or of the beneficial owner may be subject to imprisonment not exceeding 2 years and/or to a **penalty** of up to €100,000.

5.5 Identification and verification of legal entities and partnerships

5.5.1 Prospective clients which are legal entities, depending on the complexity of their organisations and structures, may pose significant difficulties in **identifying and verifying their legal existence**. Hence, firms should treat with care such prospective clients and ensure that any person purporting to act on such clients' behalf is duly authorised and has the mandate to do so and identify and verify that person.

5.5.2 Firms are required to **identify** and take reasonable measures to understand the **ownership and control structure**, duly identifying the beneficial owners of the client and documenting their findings in a diligent manner. Enquiries should also be made to confirm that the entity exists for a legitimate trading or economic purpose and that the controlling persons can be identified.

5.5.3 **Certified true copies** of the original documentation verifying the information gathered regarding clients which are legal entities, should be obtained in accordance with the provisions of the Law or the Directive. The certification of the documentation should indicate that the document is a "Certified true copy of the original", stating the certifier's name, capacity and the date of certification.

Refer to Annex III for a non-exhaustive list of documents that can be used for **verification** purposes. As noted above each firm may define the documents to be accepted for verification depending on its operations and risk appetite, without jeopardising a violation of the provisions of the Law.

5.5.4 For clients which are functioning under a **partnership** agreement, firms may need to adopt a hybrid (sections 5.4 and 5.5) approach, depending on the nature (physical or legal) of the partners involved. It must also be noted that firms should obtain a thorough understanding of the affairs and participation in the partnership, identifying and verifying any partners with significant roles in the partnership like for example General partners that may have the right to represent and/or manage the partnership.

5.5.5 Moreover, the firms should identify the principal directors/partners, **persons with significant control** and beneficial shareholders of each client legal entity, in line with the requirements for natural persons (section 5.4).

5.5.6 "Know your client" is an **on-going process**. If a firm becomes aware of changes to the client's structure or ownership, or if suspicions are aroused by a change in the nature of the business transacted, further checks should be made to ascertain the reason for the changes.

5.6 Trusts and Other similar legal arrangements

5.6.1 Various cases in the past indicated that **trusts and other similar legal arrangements** may be abused by criminals wishing to avoid the identification procedures and mask the origin of illicit funds. Particular care should to be exercised when dealing with such legal arrangements, especially when established in jurisdictions without equivalent or stricter money laundering and terrorist financing procedures, than the EU in place. The risk of money laundering and terrorist financing must be cautiously assessed and mitigated in such cases.

5.6.2 In accordance with the **beneficial owner definition** contained in the Law, all natural persons exercising ultimate control over the trust or other similar legal arrangement by means of direct or indirect ownership or by other means including the settlor(s), the trustee or commissioner, the protector(s) (if any) and the beneficiary/ies, should be identified and verified (see sections 5.4 and 5.5).

5.6.3 Additionally, where the individual(s) benefiting from the legal arrangement or legal entity have **yet to be determined**, the class of persons in whose main interest the legal arrangement or entity is set up or operates should also be known to the ICPAC member providing services to the legal arrangement. The firm should establish the identity of the beneficiary/ies at the time of a payout or at the time of the exercise by the beneficiary of its vested rights.

5.6.4 Where a firm receives **money on behalf of a trust**, it is important to ensure that the source of funds is properly identified, that the nature of the transaction is understood and that payments are made only in accordance with the terms of the trust and are properly authorized in writing by the trustee.

5.6.5 In the case of **occupational pension schemes**, the identity of the principal employer should be verified, and also (by inspecting the scheme's trust documents) that of the trustees. There is no need to verify the identity of those who are to receive scheme benefits, unless the firm is to give them advice on an individual basis.

5.6.6 Where the client is a **club, a society or a charitable foundation**, the firm should examine and find out the purpose of its operation and ensure its legality requesting the provision of its constitution and the Certificate of Registration issued by the relevant Government Authority. In addition, the firm should verify the identity of all signatories in accordance with the established procedure of verifying the identity of natural persons.

It must also be highlighted that recent studies have indicated that clubs, societies and charitable foundations may be used by criminals and more importantly terrorist financiers. Therefore, firms must be very careful when performing CDD and Risk Assessment on such structures, placing more emphasis on the purpose of the setup, the jurisdictions exposed to, as well as any suspicious associates of the clubs, societies or charitable foundations.

5.6.7 In cases where the client is a **local authority or other public body**, the firm should obtain a copy of the resolution authorising the undertaking of the relevant transaction. The individual/s dealing with the firm having the relevant authority to act, should also be identified and verified.

5.7 Enhanced Due Diligence (EDD) & PEPs

5.7.1 Each firm should clearly outline in its AML manual or CAP, the **categories** of clients for which it will be performing **EDD**, for clarity purposes. Provisions of chapter 4, section 5.7.2, as well as Annex II should be taken into account.

5.7.2 Firms should adopt a Risk Based Approach (see chapter 4) to CDD and identify circumstances in which there is a higher risk of money laundering and terrorist financing. Enhanced due diligence should be performed for higher risk categories of clients, business relationships or transactions.

The **Law specifies** that **enhanced due diligence** must be applied when transacting or establishing a business relationship with:

(a) A natural person coming from or a legal entity established in a high-risk third country
(b) A PEP (including family members and close associates)
(c) Other cases presenting high risk of money laundering and terrorist financing in accordance with the risk appetite of the firm (see chapter 4)

5.7.3 **EDD measures** for business relationships and/or transactions may include the following:

a) Looking for additional independent, reliable sources to verify information, including identity information, the integrity and the permanent address of the client (e.g. Reference letter from a reliable professional adviser in the prospective

client's home country) – See Annex III

b) Detailed examination of the background and purpose of the business relationship, to understand better the background, ownership and financial situation of the client, other associates and relevant parties
c) Increasing and customising the level and nature of monitoring of the business relationship, including greater scrutiny of transactions
d) Taking further steps to be satisfied that transactions are consistent with the purpose and intended nature of the business relationship

5.7.4 **EDD procedures** must be customised to respond to areas that pose higher risk, emanating from the business relationship with the corresponding client.

See table below for practical examples

High risk area on client profile	**EDD measures to mitigate risk**
Non-resident & non-face to face	Additional identity verification
PEP	More details and supporting documentation on source and size of wealth
High net worth client	More details and supporting documentation on source and size of wealth
Business relationship with high risk 3rd countries	More thorough and sophisticated transaction monitoring
Cryptocurrency related activities	More details on the activities, from where cryptos obtained, type of cryptos (anonymous)
CIP clients	More details and supporting documentation on source and size of wealth, background, controversies, adverse media, purpose of application and other

Special consideration should be given to complex and unusually large transactions and all unusual patterns of transactions, which may seem to have no apparent economic or lawful purpose, in order to determine whether those transactions or activities appear suspicious.

5.7.5 **High risk third countries** include any country which is widely known to face strategic deficiencies, problems of bribery, corruption and financial irregularity and whose laws and regulations for the prevention of money laundering and terrorist financing are not equivalent with international standards. A list has been issued by the European Commission and published in the Official Journal of the Union. Firms are encouraged to also use the FATF

list identifying High risk and other monitored jurisdictions, with weak measures to combat money laundering and terrorist financing.

In cases where the person coming from high risk third country belongs to a group, that adopts and implements equivalent or stricter than the EU money laundering and terrorist financing group–wide policies and procedures and evidence of full compliance is available, then the EDD requirements may not be automatically applicable. The situation will have to be assessed further.

5.7.6 Firms should put in place appropriate risk management systems and risk- based procedures to determine whether a potential client, a client or the beneficial owner is a **PEP**. Examples of measures that could form part of such risk based procedures include seeking relevant information from the client, referring to publicly available information or having access to commercial electronic databases of PEPs, always ensuring full compliance with the provisions of the Processing of Personal Data (Protection of the individual) Law.

5.7.7 More attention should be paid when the **PEPs are connected (nationality, residency, citizenship or location of business activity) with a country which is widely known to face problems of bribery**, corruption and financial irregularity and whose laws and regulations for the prevention of money laundering and terrorist financing are not equivalent with international standards.

5.7.8 ~~Firms that provide regularly services to international clients are encouraged to subscribe in a **specialist database**. Firms using specialist databases should comprehend how these databases are populated and need to ensure that those flagged by the database fall within the definition of a PEP defined above.~~ Firms must apply systematic background checks on high risk clients, as part of the enhanced due diligence process.

5.7.9 Where a business relationship with a PEP related client including family and close associates of a PEP, is established the firm should apply the following specific **EDD measures,** in accordance with the provisions of the Law:

a) Senior management officials approval for establishing a business relationship or for the continuation of business relationships with an existing client which has become a PEP,
b) Take adequate measures to establish the size and source of wealth and funds of clients
c) Conduct enhanced on-going monitoring of the business relationship

The above EDD measures may also be adopted for various high-risk clients other than PEPs.

5.7.10 Firms should continue treating natural persons as **PEPs, after they cease to hold a prominent public function**, for a period of at least 12 months. Firms should continue applying EDD measures to PEPs for more than 12 months after they have ceased to hold a prominent public function, when assessing that they present a higher risk for money laundering and terrorist financing, due to any significant influence they may still have. The above provisions apply for family members and persons that are known to be close associates of PEPs, in accordance with the Law.

5.8 Simplified Due Diligence (SDD)

5.8.1 **SDD** measures may be applied in exceptional cases. It must be highlighted though that monitoring of transactions and business relationships, to enable the detection of unusual or suspicious transactions is always required. Additionally, the obligations to report to MOKAS any identified transactions still remain.

These exceptional situations should be considered on a case by case basis, ensuring that the business relationship or transaction presents a low risk for money laundering and terrorist financing, in accordance with the guidance provided on chapter 4 and based on the content of Annex I (Low risk). The rationale behind SDD application should be clearly documented in the AML manual or CAP.

5.8.2 It is stressed that where an **STR or SAR is submitted** for a client for which SDD measures were performed, the client should be immediately re-classified to High risk. Consideration should also be made for implementation of EDD procedures in coordination with MOKAS and without jeopardising an investigation or tipping off the suspect (see section 1.5.3)

5.8.3 In **applying SDD**, CDD measures are still required but certain adjustments can be made to reflect the assessment of low risk. The adjustments mentioned above may cover the following:

a) The quality and source of information obtained for identification and verification purposes
b) The timing of application of CDD procedures
c) The frequency of scheduled or routine CDD updates referred in 5.3.2
d) The frequency and extent of transaction monitoring

5.9 Third party reliance

5.9.1 Firms may rely on third parties, by entering into an agreement with the third party, for carrying out all or part of the client identification and due diligence procedures. The agreement should explicitly state that the third party should make available to the firm copies of the CDD documentation requested immediately for the establishment of the business relationship.

Despite the above, firms should remain vigilant of such reliance as the firm will **remain liable** for any compliance failure, notwithstanding its reliance on third parties. Therefore, ICPAC firms placing reliance on third parties should satisfy themselves with the level of CDD being undertaken by the third party.

5.9.2 **Reliance for CDD** purposes may only be placed on a credit institution, a financial institution, an auditor, an external accountant, a tax advisor, a trust and company service provider or an independent legal professional that fulfils the following conditions:

a) It applies CDD and record keeping measures which are consistent with the measures pursuant to the EU Directive and

b) It is subject to supervision which is consistent with the requirements of the EU Directive.

Firms opting to rely on a third party should also make sure that the third party will make available and forward immediately data, identification documents, information or documentation obtained for CDD procedures. It is highlighted that reliance should only be placed on third parties on the **outset** and that no reliance can be placed on any third party when conducting ongoing monitoring.

Special attention should also be paid to ensure that the party to be relied upon is in full compliance with the Processing of Personal Data (Protection of the individual) Law.

5.9.3 Before accepting the information and documentation by the said third party, the firm should apply the following **additional measures**/procedures:

(a) Assess the systems and procedures applied by the third party for the prevention of money laundering and terrorist financing
(b) Satisfy itself based on the assessment of point (a) that the third party implements client identification and due diligence systems and procedures which are in line with the requirements of the Law and this Directive
(c) Maintain a separate file for every such third party, where it stores the assessment report relating to point (a) and other relevant information
(d) Take steps to ensure that the third party to be relied upon will provide copies of the original documentation immediately
(e) The commencement of the cooperation with the third party and the acceptance of client identification data verified by the third party is subject to approval by the Compliance Officer.

5.9.4 ICPAC firms are **prohibited** from **relying** on third parties established in **high-risk third countries**. A branch or majority owned subsidiary of an obliged entity established in the European Union, which is located in a High Risk country, which fully complies with group-wide policies and procedures that are consistent or stricter than the provisions of the EU directive, may be exempted from the prohibition by ICPAC.

5.9.5 Prior to granting consent to **be relied upon**, an ICPAC member must ensure that its client (and any other party whose information may be disclosed) is aware that a disclosure may be made to another party and ensure that he has no objection regarding such disclosure. It should also make sure that it can make available immediately on request, data, identification documents, information or documentation obtained during CDD procedures.

5.9.6 ICPAC firms could rely on an overseas branch office or associated firm that belongs in the same group, provided that the **group** applies common client due diligence and record keeping procedures and measures against money laundering and terrorist financing, consistent or stricter with the provisions of the EU Directive and the effective application of such measures and procedures is supervised at group level by a competent authority of the home member state or of the third country.

5.9.7 Where a firm **merges with another firm**, or acquires the practice of another firm in whole or in part, it may not be necessary for the identity of clients of the merged or acquired practise to be re-verified, provided that satisfactory identification records are available.

5.10 Outsourcing arrangements

5.10.1 Where a firm is engaged by another party, X, to assist with an engagement X has with another party, Y, then the ICPAC member should carefully consider and document who its client is. Where there is no business relationship formed and hence no engagement letter in place between the ICPAC member and Y, then CDD on Y may not be required. Instead CDD on X should be obtained.

In a different scenario, Y is also deemed as a client and CDD should also be obtained, where there is a business relationship established with Y and hence there is significant contact. Similar considerations apply in **networked arrangements**, where work is referred between member firms of the same network.

5.11 Clearance letter

5.11.1 A firm which is taking over a professional appointment replacing an existing auditor, external accountant, tax advisor, trust and company service provider, insolvency consultant or other advisor, should come in contact with their predecessor. This can provide evidence for the identity as well as the integrity of the client, and is therefore a valuable procedure in this context. A **clearance letter** should be obtained from the predecessor, stating whether there are any Money Laundering and/or Terrorist Financing issues on the concerned client.

6 Ongoing monitoring of transactions and business relationships

6.1 Ongoing monitoring procedures

6.1.1 **Ongoing monitoring** is a vital part of effective Anti-money laundering and counter terrorist financing compliance systems. Ongoing monitoring procedures assist obliged entities to update existing knowledge on their clients and detect any unusual or suspicious activities.

Ongoing monitoring procedures should be customised depending on the type of services offered to the client. An audit client's ongoing monitoring procedures should differ from the monitoring procedures adopted for a client that obtains directorship or bank management services.

6.1.2 For example, a firm can perform **ongoing monitoring** by:

(i) Reviewing the documents and information collected for CDD purposes relating to the client, to ensure they are up-to-date, relevant and certified in accordance with the provisions of Annex III

(ii) Examining transactions carried out by the client or on behalf of the client, to ensure that they are consistent with the existing knowledge of the clients' functions, business, risk profile and size and source of funds and/or wealth (economic profile of client)

(iii) Identifying complex transactions, unusually large in amount or of an unusual pattern or that have no apparent economic or lawful purpose which may indicate money laundering and/or terrorist financing

(iv) Making appropriate inquiries of clients

6.1.3 When **examining transactions** an ICPAC member may consider for example the following **factors**:

(a) Geographical source/destination of funds
(b) High or inconsistent amounts
(c) Numerous small transactions that when combined they exceed anticipated threshold
(d) Nature or type of individual transactions or series of transactions
(e) Clients' usual pattern of activities or size of turnover
(f) Changes in the usual method of communication with client
(g) STRs or SARs

6.1.4 In cases where the substance of a business relationship changes significantly, firms should perform additional CDD procedures to identify and subsequently mitigate the money laundering and terrorist financing risks involved. If the revised risk is not in line with the Client Acceptance Policy of the firm, then consideration should be made to terminate the business relationship.

Changes in the terms of a business relationship with clients may include amongst others, the following:

(a) Changes in the shareholding structure
(b) Changes in the activities or turnover of a client that do not have commercial rationale
(c) Enquiries and provision of new higher risk services
(d) Changes in the nature of transactions of a client that cannot be explained
(e) Set up of new corporate structures

It is noted that the above list is not exhaustive.

Depending on the findings of ongoing monitoring procedures, firms should consider the reclassification of a client risk profile and subsequently the application of risk appropriate due diligence measures.

6.1.5 Sufficient **guidance** must be given **to staff members** to enable them to perform effective monitoring.

6.2 Risk-based approach application on ongoing monitoring

6.2.1 Ongoing monitoring may be **proportional to the risk** profile of the client. The higher the risk of a client the more frequent and more rigorous the monitoring procedures should be. Particular attention on ongoing monitoring procedures must be paid in client relationships where a PEP is involved or where a client has any links or relationships with high risk countries. By adopting a proportional to risk approach, firms can utilise their resources more effectively.

6.2.2 Despite the proportionality principle mentioned above, it must be noted that ongoing monitoring should take place for **all client relationships** including low risk clients and clients for which Simplified Due Diligence measures were adopted. What can be altered accordingly is the frequency and extent of the ongoing monitoring.

6.2.3 Firms may consider, depending on the size, nature and type of service offered the **use of software** for more efficient transaction monitoring.

7 Terrorist Financing

7.1 Funding of terror

7.1.1 **Funding of terrorist organisations** is made from revenue generated by both legal and illegal activities.

7.1.2 **Legal fund raising methods** used by terrorist groups include:

(a) collection of membership dues and/or subscriptions,
(b) sale of books and other publications,
(c) cultural and social events,
(d) donations,
(e) community solicitations and fund raising appeals.

7.1.3 As noted above, **funds obtained from illegal sources** are also used by terrorist groups. These include cash smuggling by couriers or bulk cash shipments, structured deposits to or withdrawals from bank accounts, use of hawala network, purchases of financial instruments, wire transfers by using “straw men”, false identities, front and shell companies as well as nominees from among their close family members, friends and associates. Criminal activities generating such proceeds may include but not limited to kidnappings (requiring ransom), extortion (demanding “protection” money), smuggling, thefts, robbery, drug trafficking and illegal oil trafficking.

7.1.4 The scope of terrorists is to conceal how the money will be used and where it originated. Funds may also come from illegal sources, which appear legal through money laundering. Even though the most important role in combating the financing of terrorism is played by financial institutions, all obliged entities which participate in the chain of provision of services, such as tax advisors, accountants, auditors, lawyers, insurance companies, car dealers etc., should be engaged in this effort. Emphasis should be placed on the **connections and network of the client** in such situations.

7.1.5 **Non–profit and charitable organisations** are also used by terrorist groups as a means of raising funds and/or serving as cover for transferring funds in support of terrorist acts.

The potential misuse of non-profit and charitable organisations can be made in the following ways:

a. Establishing a non-profit organisation with a specific charitable purpose but which actually exists only to channel funds to a terrorist organisation.
b. A non-profit organisation with a legitimate humanitarian or charitable purpose is infiltrated by terrorists who divert funds collected for an ostensibly legitimate charitable purpose for the support of a terrorist group.
c. The non-profit organisation serves as an intermediary or cover for the movement of funds on an international basis.
d. The non-profit organisation provides administrative support to the terrorist movement.

Unusual characteristics of non-profit organisations indicating that they may be used for an unlawful purpose are the following:

a. Use of funds by a non-profit organisation is not consistent with the purpose for which it was established.
b. Donations relating to a cause that is subject to derogatory publicly available information (crowdfunding initiative, charity, NPO, NGO, etc.).
c. A mismatch between the type and size of financial transactions and the stated purpose and activity of the non-profit organisation.
d. A sudden increase in the frequency and amounts of financial transactions for the account of a non-profit organisation.
e. Large and unexplained cash transactions by non-profit organisations.
f. The absence of contributions from donors located within the country of origin of the non-profit organisation.

7.1.6 The following actions shall be deemed to be **terrorist offences**:

a. attacks upon a person's life which may cause death,
b. attacks upon the physical integrity of a person,
c. kidnapping or hostage taking,
d. causing extensive destruction to a Government or public facility, a transport system, an infrastructure facility, including an information system, a fixed platform located on the continental shelf, a public place or private property likely to endanger human life or result in major economic loss,
e. seizure of aircraft, ships or other means of public or goods transport,
f. manufacture, possession, acquisition, transport, supply or use of weapons, explosives or of nuclear, biological or chemical weapons, as well as research into, and development of, biological and chemical weapons,
g. release of dangerous substances, or causing fires, floods or explosions the effect of which is to endanger human life,
h. interfering with or disrupting the supply of water, power or any other fundamental natural resource the effect of which is to endanger human life,
i. threatening to commit any of the acts listed in (a) to (h).

Combating the Financing of Terrorism (CFT) involves investigating, analyzing, deterring and preventing sources of funding for activities intended to achieve political, religious or ideological goals through violence and the threat of violence against civilians. By tracking down the source of the funds that support terrorist activities, law enforcement may be able to prevent some of those activities from occurring. Instead of trying to catch a criminal plotting or committing an act of terrorism through other means such as surveillance, law enforcement addresses the problem from the money side by detecting suspicious financial transactions and tracking down all the individuals and organisations involved in those transactions.

7.1.7 Firms should fully adhere to the requirements of this Directive and **apply proper risk assessment measures and procedures**, in line with the ICPAC Guidance Paper on Risk Based Approach (RBA).

8 Record Keeping and Data Protection

8.1 Record keeping

8.1.1 Firms must retain the following records and information for a period of five years after the end of a business relationship with a client or after the date an occasional transaction was completed:

(a) Copies and information for compliance with the Client Due Diligence (CDD) requirements covered in chapter 5
(b) Evidence and records of transactions both domestic and international
(c) Correspondence documents with clients
(d) Suspicious Transaction Reports and/or Suspicious Activity Reports performed by staff members including the examination performed by the CO, the corresponding findings and any subsequent communication with **MOKAS**.

Records and information retained must be visible, legible and of sufficient content and quality, to permit reconstruction of transactions so as to provide, if needed, evidence for prosecution of criminal activity. It is highlighted that processes should be established, for the retrieval of records and information retained, which must be accessed timely and without due delays.

In cases where it is reasonably justified, firms should retain records and information for five additional years, bringing the total retention period to a maximum of ten years after the end of a business relationship with a client or after the date an occasional transaction was completed. Reasonable justification refers to the prevention, detection and investigation of Money Laundering and Terrorist Financing in relation to ongoing criminal proceedings or suspicions.

Firms should establish, maintain and implement a **record retention policy** reflecting the provisions of the Law and other applicable legislation, including GDPR. In the record retention policy, the firms may categorise/classify the types of records kept, allocating to each category/classification a retention period. Firms should ensure that record retention and data protection requirements are applicable to electronic and paper-based records and information.

8.1.2 Firms should ensure that all information outlined in section 8.1.1, become available promptly to **MOKAS and the Institute**, when needed for the purpose of execution of their duties.

It is noted that firms may use electronic files of KYC documents (Passport copies, Utility bills, corporate documents and others) in their daily functions but upon request by MOKAS, ICPAC or any other competent authority, they should present the original documents or certified true copies of the original documents.

8.1.3 An ICPAC member that is part of a Group that implements **group-wide policies** on record retention and data protection policies for the purpose of prevention of money laundering and terrorist financing, must confirm that these policies are in full compliance with the provisions of the Law, ensuring that the minimum requirements in the corresponding locations and/or jurisdictions are at least as strict as the provisions of the Law and present Directive.

Additionally, it should ensure that the above mentioned policies are implemented effectively in all branches and subsidiaries in member states and third countries.

In cases where the legislation in the third country does not permit application of policies and procedures equal or stricter from the provisions of the Law, then the member of ICPAC must inform the Institute and take additional measures to mitigate the increased risk of money laundering and terrorist financing.

8.1.4 In the event where any person during the performance of the procedures for client identification and due diligence measures, knowingly provides false or forged or misleading evidence or information for the identity of the client or of the beneficial owner may be subject to imprisonment not exceeding 2 years and/or to a **penalty** of up to €100,000.

8.2 Data Protection

8.2.1 Firms should always act in accordance with the provisions of the applicable data protection legal and regulatory framework, including Regulation (EU) 2016/679 (General Protection Regulation) **("the GDPR")** and the Law on the Protection of Natural Persons Against Personal Data Processing and the Free Movement of Such Data of 2018 (L.125(I)/2018) ("the Personal Data Protection Law").

The collection and further processing of personal data by ICPAC members, to fulfil their AML and Compliance obligations emanating from the Law, is considered a matter of public interest. Firms should ensure however, that the collected personal data is not used in any other way nor subjected to any commercial or other incompatible processing. Any sort of incompatible processing may be considered a violation.

8.2.2 Firms should inform their potential clients prior to initiating a new client relationship or the execution of an occasional transaction, of the **type of data** required to fulfil their AML and Compliance obligations (e.g. Name of client, Residential address of client etc.). In addition, firms should communicate with clarity the legal basis (or bases) of processing as well as the **type of processing** the firm will perform with the collected information, in accordance with the GDPR.

8.2.3 Firms should also inform their potential and existing **clients** of the **rights** conferred to them via Articles 15, 16, 17, 18 and 20 of the GDPR, and provide them with specific steps and contact details (such as the Firm's Data Protection Officer) so that such potential and existing clients can exercise those rights.

8.2.4 Firms should clearly explain that the rights referred to in 8.2.3 above are not absolute, especially in relation to the need to avoid jeopardising money laundering and/or terrorist financing inquiries, analyses or investigations. Similarly, clients should be informed that their right to erasure ("**right to be forgotten**") may not be exercised at an earlier time than the period mentioned in section 8.1.1, since that will consist a violation of the provisions of the Law.

8.2.5 In addition, firms should refrain from carrying out transactions which they know or suspect to be related with money laundering or terrorist financing, before they **inform MOKAS.** If it is considered impossible to refrain from carrying out the transaction or is likely to disturb efforts of an operation to track suspects of money laundering or terrorist financing, ICPAC members, must inform MOKAS immediately afterwards.

9 Suspicious Transaction & Activity Reports (STRs & SARs)

9.1 Statutory requirements

9.1.1 In accordance with the Law, all obliged entities including ICPAC firms should implement internal reporting procedures enabling all employees to report and disclose any information or other matter that creates reasonable suspicions of Money Laundering and Terrorist Financing (STRs & SARs). A senior member of staff must be appointed as Money Laundering Compliance Officer also known as **Compliance Officer** (See chapter 3), to whom all internal STRs and SARs including other information should be addressed and disclosed. Failure to file an STR and/or SAR and disclose such information or other matters may result in penalties to both the individual and the firm. See section 1.5.5 for details on the penalties.

9.1.2 It is noted that once an employee reports his suspicion to the Compliance Officer, then he is considered to have fully satisfied his statutory obligations as far as reporting STRs and SARs are concerned. It should be made absolutely clear to the members of staff filing a suspicion report, to refrain from tipping off the suspect (see section 1.5.3) and ensure that in case additional information or assistance is requested by MOKAS this is provided promptly.

All **internal STRs & SARs** made to the Compliance Officer by members of staff **must be examined carefully** by the Compliance ~~Department~~ Officer taking into consideration any other relevant information and determine whether or not the STR/SAR should be reported to MOKAS.

9.1.3 Upon conclusion of the examination, the Compliance Officer should document the details of the case and if needed to report to MOKAS immediately. It must be highlighted that **reports to MOKAS** must also include identified or suspected attempts to carry out Money Laundering and Terrorist Financing and not only suspicions about transactions or activities that already took place.

9.1.4 The above **provisions do not apply** in appointments to ascertain a client's legal position or defend them in legal proceedings.

9.1.5 Any disclosure of STRs or SARs made in **good faith** shall not constitute a breach of any contractual obligation or confidentiality agreement between the firm and its client. Consequently, such an event will not give rise to any liabilities on behalf of the directors and/or employees of the firm.

9.1.6 Using the same principle outlined in section 9.1.5, any person who submits an STR or SAR (both internal and towards MOKAS) is **protected from being exposed** to threats or hostile action as well as adverse or discriminatory employment actions.

9.1.7 Firms should include in their **engagement letters** a paragraph notifying clients of the firm's potential reporting obligations emanating under the Law. Firms may use a general form of wording, which would extend to other matters where reporting to regulators for instance is required. It may also be useful to include a statement that Cyprus law will govern the provision of the firm's services and that the Cypriot courts will have an exclusive jurisdiction over any dispute.

9.2 Recognition of suspicious transactions and activities

9.2.1 A suspicious transaction or a suspicious activity will often be inconsistent with a client's known legitimate business or personal activities or with the normal business for that type of client. Hence, in depth **knowledge of the client's business** is fundamental to enable a person to recognise that an activity, a transaction or a series of transactions is unusual or suspicious. The Institute released Guidance Notes on Suspicious Transactions/Activities providing additional insight on the subject.

9.2.2 "**Red flags**" are the indicators that an established client's transactions or activity might be suspicious or related to money laundering and/or terrorist financing.

Some red flags may include the following (the list is not exhaustive):

(a) The size of the transaction (or transactions when aggregated) is inconsistent with the normal activities of the client documented in the economic profile
(b) The pattern of transactions conducted by the client has changed
(c) The transaction is unnecessarily complex or unusual with no visible economic or commercial rational
(d) The transaction is not rational in the context of the client's activities documented in the economic profile
(e) The transaction is international in nature and the client has no obvious reason for conducting business with the other country involved

A list containing examples of red flags, which can be used as guidance for assisting a firm and its employees in recognising suspicious transactions, can be found in Annexes IV and V.

9.2.3 Sufficient and adequate **guidance** and training must be given **to staff** enabling them to recognise suspicious transactions. The type of situations giving rise to suspicions will depend on a firm's client base and range of services and products. A firm may also consider monitoring the types of transactions and circumstances that have given rise to suspicious transaction reports by staff, with an objective of updating internal instructions and guidelines from time to time.

9.3 Internal reporting procedures

9.3.1 A firm should make the necessary arrangements in order to introduce measures designed to assist the functions of the Compliance Officer and the **reporting of suspicious transactions by employees**.

Firms have an obligation to ensure that:

(a) All their employees know to whom they should report a money laundering and/or terrorist financing knowledge or suspicion and
(b) There is a clear reporting chain under which money laundering and/or terrorist financing knowledge or suspicion is passed without delay to the Compliance Officer.

9.3.2 **Reporting lines** should be as direct and short as possible. The person with the suspicion should be able to reach directly the Compliance Officer. This ensures speed, confidentiality and accessibility to the Compliance Officer. All members of staff of firms should also be aware that they have a direct route to the Compliance Officer.

9.3.3 Larger firms may choose to appoint **assistant Compliance Officers** within departments or branch offices, to enable the validity of the suspicion to be examined before being passed to the Compliance Officer of the firm. The assistant Compliance Officer's role must be clearly specified and documented in the firm's corresponding manual.

9.3.4 All **suspicions reported** to the Compliance Officer should be documented (in urgent cases this may follow an initial discussion by telephone). It is also possible in some cases for a member of staff to discuss the suspicion with the Compliance Officer and prepare the report jointly. The report should include full details of the client and full description of the information giving rise to the suspicion.

9.3.5 The Compliance Officer should **acknowledge receipt** of the report and at the same time provide a reminder of the obligation to avoid "tipping off" (See section 1.5.3). All internal enquiries made in relation to the STR or SAR, and the reason behind whether or not to submit the report to MOKAS, should be clearly documented. This documentation may be used as evidence of good practice and due diligence for the firm, if there is an investigation and the suspicions are confirmed in the future. See section 1.5.4 for details.

9.3.6 The Compliance officer should immediately consider whether the firm should keep the client (always in coordination with MOKAS where needed) and/or **re-classify the reported client to High risk** and hence use EDD measures.

9.3.7 The firm may consider **providing feedback** to the reporting person, department or branch office of the decision taken by the Compliance Officer, particularly if the reported suspicions are believed to be without ground. Likewise, at the end of an external investigation, consideration should be given to advise all members of staff concerned of the outcome. It is particularly important that the Compliance Officer is informed of all communications between the investigating officer and the firm at all stages of the investigation. For more details on the role of the Compliance Officer, see Chapter 3.

9.3.8 Records of suspicions which were raised internally with the Compliance Officer but not disclosed to MOKAS and/or the law enforcement agencies should be **retained for at least five years** from the date of the transaction.

9.4 Reporting to MOKAS

9.4.1 All STRs or SARs reported to MOKAS should be submitted through the GoAML platform via the following web address https://reports.mokas.law.gov.cy/live/Home. Any subsequent information or documentation judged appropriate to be shared with or asked by MOKAS, must be submitted as an Additional Information File (AIF) via the GoAML.

9.4.2 MOKAS issued **guidance notes** for obliged entities covering the submission of STRs and SARs which can be found on the Institute's website. More specifically the guidance covers the following areas:

(a) Method of reporting to MOKAS
(b) Basic structure of STRs and SARs
(c) Accurate and descriptive suspicion
(d) Diligent completion of GoAML platform fields
(e) STRs and SARs
(f) Supporting documentation disclosure
(g) Orders for disclosure of information
(h) Communication with the FIU

9.4.3 ICPAC firms are **encouraged to register** on GoAML platform following the MOKAS registration instructions and familiarise themselves with the reporting process. In case of a real reportable incident, the firm will be in an advantageous position if already familiarised with and registered on the platform, since valuable time will be saved. Upon registration on the GoAML platform, ICPAC firms will also be able to receive directly relevant circulars by MOKAS.

9.4.4 MOKAS may inform obliged entities who submitted a STR/SAR where practicable, on the **effectiveness of the ~~investigations~~ SARs/STRs as well as monitoring reports** via GoAML system or other means.

9.5 Confidentiality

9.5.1 The Law protects those reporting suspicions of money laundering or terrorist financing from claims in respect of any alleged breach of **confidentiality,** including threats or hostile action. This ensures that no action can be taken against the reporter even where the suspicions are later proved to be ill founded. However, the protection extends only to disclosure of the suspicion or belief that funds derived from money laundering or terrorist financing, and to matters on which that suspicion or belief is based. If in doubt, firms should insist on the law enforcement agencies obtaining a court order before disclosing information beyond that contained in their initial report.

9.5.2 In the event of a prosecution, the **source of the information** provided to MOKAS is **protected**, as far as the rules for the disclosure of evidence allow. Maintaining the integrity of the confidential relationship between law enforcement agencies and firms, is considered by MOKAS to be of paramount importance. The origins of financial disclosures are not revealed because of the need to protect the disclosing firm and to maintain the confidence in the disclosure system.

9.6 Constructive trust

9.6.1 The duty to report suspicious transactions and to avoid "tipping off" can lead to a conflict between the reporting firm's responsibilities under the criminal law, and its obligations under the civil law as a **constructive trustee**, to a victim of fraud and other crimes.

9.6.2 Where a firm comes to know that property belongs to a person other than its client, it can become a constructive trustee of that property and, therefore, **accountable** for it **to its true lawful owner**.

The most likely cases when a firm might know, that property belongs to a third party other than its client, are outlined below:

(a) The firm receives property and deals with it in a way which he knows to be inconsistent with the rights of the true owner. Special attention must be paid to the fact that the firm may be acting with the consent of the law enforcement agencies. Despite that, this would not be a defence to a claim by the true owner.
(b) The firm does not itself receive the property, but it acts in a way which it knows will assist others to defraud the true owner of this property.

"Knows" has a wide meaning in the above context. Even if a firm has no actual knowledge, it could still be liable to the true owner, if it should have known that his rights were being or might be infringed.

9.6.3 A firm's liability as a constructive trustee arises when it comes to know that assets rightfully belong to a person other than its client. The firm then takes on the **obligation of constructive trustee** for the true lawful owner. If the assets are dealt with in a way which is inconsistent with the rights of the true lawful owner, the civil law treats the firm as if it were a trustee for the assets, and may hold the firm liable to restore the losses suffered. Having a suspicion which is considered necessary to report under the money laundering and terrorist financing legislation, could be taken as an indication that the firm knows or ought to have known under the specific circumstances that the assets belong to a third party.

9.6.4 In the normal course of events, a firm would not dispose assets to a third party knowing itself to be in breach of trust. The money laundering or terrorist financing suspicion must be reported by the firm to MOKAS always in accordance with Law. The firm may need to act on the client's instruction, after requesting and receiving the MOKAS instructions to that effect, because by refusing to hand over the assets it might alert the perpetrator of, for example a fraud, and in doing so commit a tipping off offence under the Law.

Given the absolute nature of the prohibition in the criminal law, if a firm makes a disclosure under the Law, and is acting in accordance with the instructions of MOKAS or the investigating officer in disposing of the assets, one may wrongfully regard the **risk** of the firm **being held liable** by a civil court as constructive trustee, to be low.

9.6.5 In order to truly **minimise the liability** derived from a possible constructive trusteeship described in 9.6.4, the following procedures should be followed:

(a) When evaluating a suspicious transaction, the CO should consider whether there is a constructive trust issue involved. If the CO concludes that there is a reason to believe that the firm may incur a liability as a constructive trustee, the reasons for this belief should be reported to MOKAS immediately. The constructive trust aspects should be set out clearly, with "Potential Constructive Trust Issue" marked clearly at the top of this section. Neither the client nor any third party should be tipped off.

(b) On receipt of the report, MOKAS will evaluate the information and "fast track" the report to the appropriate investigator who will determine whether the "consent" to undertake the transaction can be issued.

(c) Where a suspicious transaction report has previously been made to MOKAS, and a potential constructive trust issue comes to light subsequently, the FIU (or the designated investigator) should be provided with an immediate Additional Information File (AIF) report, indicating the reasons why a constructive trust situation is believed to have arisen.

9.6.6 Unless entirely confident that liability as constructive trustee cannot arise, a firm should take as soon as practically possible **legal advice**.

It is essential to note that in all cases where a person knows or suspects that another person is engaged in money laundering or terrorist financing and the information or other matter on which that knowledge or suspicion is based came to his attention in the course of his trade, profession, business or employment, there is an obligation to disclose the information or other matter to MOKAS as soon as is reasonably practicable after it comes to his attention.

Failure to make such a disclosure is a serious criminal offence punishable with up to 2 years imprisonment and/or a criminal fine not exceeding €5,000 as per section 27(4) of the Law (See section 1.5.5). Therefore it is never appropriate to delay making a disclosure to MOKAS pending an application to the court for directions. Firms must report the matter to MOKAS as soon as reasonably practicable. A member of the Institute in such a position should inform MOKAS of the sensitive nature of his obligations as constructive trustee and should take legal advice as soon as practically possible.

10 Training and awareness

10.1 Statutory Requirements

10.1.1 All ICPAC firms should take appropriate measures to **inform their staff** members, of the Law, the ICPAC Directive and all EU Directives on Anti money Laundering and Terrorist financing. Firms should also ensure that members of staff are aware of and familiarized with the policies and procedures referred in section 2.1 of this Directive, as well as the relevant provisions of the Processing of Personal Data (Protection of the Individual) Law. It is good practice for firms to ensure that all staff members have read the AML manual of the firm and confirm that they understand its content.

10.1.2 Firms should also ensure that all staff members are always updated with the most recent developments and are provided **ongoing training**, enabling them to recognise and handle transactions and activities which may be related to Money Laundering and Terrorist Financing.

10.2 Need for awareness

10.2.1 Staff should be aware of the background on which the Law is enacted and be fully aware of their responsibilities and personal statutory obligations. Employees of an ICPAC firm should also be aware that they may be **personally liable** for failing to report information in accordance with the firm's internal procedures.

10.2.2 All staff must therefore be trained to recognize **red flags** (Section 9.2.2, Annex IV and Annex V) and encouraged to alert the Compliance Officer of any knowledge or suspicion of transactions or activities involving money laundering or terrorist financing. It is highlighted that firms must introduce comprehensive measures to ensure that their staff is fully aware of their responsibilities for identification and reporting of suspicious transactions.

10.2.3 Training procedures should also cover the importance of Client Due Diligence (**CDD**) and Know Your Client (**KYC**) in relation to monitoring the business relationship, as well as the specific transactions of the client. It must be emphasised not to hesitate enquiring with clients and corroborate on transactions ensuring that enough information is gathered about the type of business activities expected in relation to that client at the outset, so as to know what might constitute suspicious activity at a future date. Relevant staff should be trained to be cautious and identify any change in the pattern of a client's transactions or circumstances that might relate to Money Laundering and/or Terrorist Financing.

10.3 When and how the training should be completed

10.3.1 The timing, content and methods of training for the various levels/types of staff should be **tailored** to meet the needs of the particular firm, depending on the size and nature of the organisation.

10.3.2 The **frequency** of trainings should be determined taking into consideration key factors like changes in the legislation, regulation, professional guidance (domestic and international), the business' risk profile, procedures, service lines and other.

10.3.3 It is necessary to have arrangements for **refresher trainings** at **regular** intervals so that the staff do not forget their responsibilities and are kept informed of any new developments in the prevention of money laundering and terrorist financing. Training sessions should also include practical examples money laundering methods used and current trends. It may not be judged necessary to repeat a complete training program regularly, but instead it may be appropriate to provide staff members with more specialised training on new or weakness areas.

10.3.4 **Training** can be delivered using various **methods** like for example face-to-face, self-study, e-learning, video presentations, other or a combination of the above. It is noted that all ICPAC members have access to the Compliance e-learning platform via the Institute website, which is specifically designed for basic needs of the members of the Institute. It is highlighted once again though, that training programs should be tailored to each firm according to its size and nature of business, as well as type of clientele. A system of tests, or some other method obtaining assurance on the effectiveness of the trainings, should also be considered. It is noted that awareness can also be raised via emails, newsletters, guidance notes, periodic team meetings and other means that facilitate the sharing of information.

10.4 Differentiation of training

10.4.1 As noted in section 10.3.1 when designing the training sessions, consideration should be given to the various levels/types of staff. Outlined below are some basic categories which could be considered for **grouping and customisation**. Each firm may adjust the design of the training according to its own organisation structure.

10.4.2 **New professional staff** that will be dealing with clients or their affairs, irrespective of the level of seniority, must obtain a general appreciation of the background on money laundering or terrorist financing, CDD and KYC procedures and of the procedures for identifying and reporting any suspicious transactions to the Compliance Officer. New staff should be made aware that suspicious transactions reporting is also their personal obligation as individuals.

10.4.3 **Front line staff** who deal directly with clients are likely to be the first point of contact with potential money launderers or terrorist financiers, and their efforts are therefore vital to the firm's reporting system. Training should be provided on factors that may give rise to suspicions and on the procedures to be adopted when a transaction or activity is deemed to be suspicious. Special emphasis should be given to the fact that this group of staff is the "eyes and ears" of the firm, that can identify any abnormal behaviour or patterns of the client.

10.4.4 **Staff who can accept clients** must receive the training recommended for front line staff. In addition, the need to verify the identity of the client must be understood, and training should be given on the firm's client verification procedures. Such staff should be aware of the types of suspicious information that may need to be reported to the Compliance Officer like forged documents, sanction related information, inconsistent activities with client economic profile and other. They must also know what procedures to follow in these circumstances.

10.4.5 **Top level management** that have the responsibility for supervising or managing staff should be provided with a higher level of instruction covering all aspects of money laundering or terrorist financing.

Firms may consider the following non exhaustive list of training areas for senior management:

(a) Recognition of a valid court order requiring information, and the circumstances when information should be declined without such an order
(b) Internal reporting procedures
(c) Requirements for verification of identity and the retention of records
(d) Offences and penalties arising under the Law for non-reporting and for assisting money launderers or terrorist financiers
(e) Red flags and recent trends on suspicious client behaviour, activities patterns
(f) Upcoming legislations or directives
(g) Recent developments

10.4.6 The **Compliance Officer** must receive in-depth training concerning all aspects of the Law, this Directive and recent developments on the field, enabling him to update internal procedures in an effective manner. In addition, the Compliance Officer should receive extensive initial and on-going training on the validation and reporting of suspicious transactions, on the feedback arrangements and on new trends and patterns of criminal activity. Reference to the training of the Compliance Officer is also made on section 2.700 paragraph 4(9) of the ICPAC Member's handbook. It is highlighted that there is an annual requirement for **10 specialised CPD units**, relevant to their Compliance functions Further advice or assistance can be obtained from compliance and Anti money laundering experts or the Institute, being the Supervisory authority.

10.5 Compliance culture

10.5.1 When designing trainings, firms should always aim to create an AML **compliance culture** within the organisation, avoiding tick the box approaches and always paying special attention to the risk-based approach. The development of a compliance culture within the firm is the strongest and most important safeguard an organisation can have in the fight against money laundering, terrorist financing and financial crime.

ANNEX I – Lower risk

Non-exhaustive list of factors and types of evidence of potentially lower risk:

1. **Customer risk factors:**
   (a) 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
   (b) public administrations or enterprises
   (c) customers that are resident in geographical areas of lower risk as set out in paragraph (3)

2. **Product, service, transaction or delivery channel risk factors:**
   (a) life insurance policies for which the premium is low
   (b) insurance policies for pension schemes if there is no early surrender option and the policy cannot be used as collateral
   (c) a pension or similar scheme that provides retirement benefits to employees, where contributions are made by way of deduction from wages and the scheme rules do not permit the assignment of a member's interest under the scheme
   (d) financial products or services that provide appropriately defined and limited services to certain types of customers, so as to increase access for financial inclusion purposes
   (e) products where the risks of money laundering and terrorist financing are managed by other factors such as purse limits or transparency of ownership such as certain types of electronic money

3. **Geographical risk factors:**
   (a) Member States of the European Union
   (b) third countries having effective AML/CFT systems
   (c) third countries identified by credible sources as having a low level of corruption or other criminal activity
   (d) third countries which, on the basis of credible sources such as mutual evaluations, detailed assessment reports or published follow-up reports, have requirements to combat money laundering and terrorist financing consistent with the revised FATF Recommendations and effectively implement those requirements.

Source: The Prevention and Suppression of Money Laundering and Terrorist Financing of 2007 as updated up until 2019

ANNEX II – Higher risk

a) Non-exhaustive list of factors and types of evidence of potentially higher risk:

1. Customer risk factors:

(a) the business relationship is conducted in unusual circumstances
(b) customers that are resident in geographical areas of higher risk as set out in paragraph (3)
(c) legal persons or arrangements that are personal asset-holding vehicles
(d) companies that have nominee shareholders or shares in bearer form
(e) businesses that are cash-intensive
(f) the ownership structure of the company appears unusual or excessively complex given the nature of the company's business

2. Product, service, transaction or delivery channel risk factors:

(a) private banking
(b) products or transactions that might favour anonymity
(c) non-face-to-face business relationships or transactions, without certain safeguards, such as electronic signatures
(d) payment received from unknown or unassociated third parties
(e) new products and new business practices, including new delivery mechanism, and the use of new or developing technologies for both new and pre-existing products

3. Geographical risk factors:

(a) without prejudice to Section 64 (1) (a) of the Law, countries identified by credible sources, such as mutual evaluations, detailed assessment reports or published follow-up reports, as not having effective AML/CFT systems
(b) countries identified by credible sources as having significant levels of corruption or other criminal activity
(c) countries subject to sanctions, embargos or similar measures issued by, for example, the European Union or the United Nations
(d) countries providing funding or support for terrorist activities, or that have designated terrorist organisations operating within their country.

Source: The Prevention and Suppression of Money Laundering and Terrorist Financing of 2007 as updated up until 2019

b) Risk Factors as highlighted by FATF:

1. The client's and the client's beneficial owner's business or professional activity, i.e. whether the activity carries a high risk of corruption (e.g. arms dealing), whether it relates to high levels of cash, whether they are regulated, etc.
2. The client's and the client's beneficial owner's reputation i.e. is there adverse media surrounding the client and the beneficial owners, are they subject to previous suspicion report or have they been convicted, etc.
3. The client's and the client's beneficial owner's nature and behaviour i.e. are they unnecessarily secretive, is their doubt of the veracity of the KYC documents, is there frequent and inexplicable change in ownership, etc.
4. The client's structure, i.e. is the structure non-transparent, unusually complex with no reasonable explanation, etc.
5. Individuals subject to sanctions issued by the U.N., EU and OFAC.
6. The level of transparency the service/transaction affords, i.e. do these services promote anonymity, do firms accept instructions given by a third party, etc.
7. The complexity of the service/transaction, i.e. whether the transactions involve a number of parties from a number of jurisdictions.
8. The value or size of the service/transaction, i.e. whether the services cash intensive or involve high value transactions.
9. Countries not having adequate AML/CTF systems e.g. FATF and EU high-risk third country lists.
10. Countries subject to sanctions, embargoes or similar measures issued by, for example the U.N., EU and OFAC.
11. Countries having significant levels of corruption or other criminal activities such as narcotics, arm dealing, human trafficking, illicit diamond trading, etc.
12. Countries identified to support terrorist activities, or have designated terrorist organizations operating within their country.
13. The channels through which the Licensed Firm establishes a business relationship or through which transactions are carried out. Channels that favour anonymity increase the risk of ML/TF if no measures are taken towards this.
14. In the cases where interaction with the client takes place on a non-face to face basis, technological measures can be put in place to mitigate the heightened risk of identity fraud or impersonation present in these situations. These measures allow a Licensed Firm to establish whether the client providing the relative identification details is actually the person he alleges to be.

c) Other factors

1. Services related to the Cyprus Investment Programme

ANNEX III - CDD Measures – Verification and certification

Client identification
The full name (including other names used), date of birth and residential address (the address at which the person can be located) should be obtained. Additional information like his source and size of wealth, Tax residence, Tax identification number, signature, his profession or occupation and any other relevant information should be obtained where relevant.

Client Verification
A document issued by an official body (e.g., government) is deemed to be independent and reliable source, even if provided by the client. Documents obtained should be valid, recent up to 6 months and certified in accordance with the provisions of section 5.4.4.

Documents found online should not be accepted if there is any suspicion regarding the origin or integrity of the documents. In cases where documents found online will be used in the client due diligence process, these documents should be annotated in accordance with section 5.4.5.

Natural Persons

The following is a suggested non-exhaustive list of sources of evidence.

Type of information	**Source of verification**
Full name & Date of birth	Certified true copy of the original: 1. Valid International Passport, or 2. Valid driving license, or 3. National ID Card It is noted that the document obtained must contain the person's photograph.
Residential Address	Certified true copy of the original: 1. Recent up to 6 months utility bill (mobile telephone line shall not be accepted), or 2. Recent up to 6 months Bank statement (stating the residential address and not the billing address), or 3. Tax Assessment, or 4. Residence permit
Source and Size of wealth and Funds (where applicable)	1. CV and/or 2. Memo prepared by the person in charge based on public search through the internet from credible websites, and public registers and/or 3. Appropriate supporting documentation (e.g. Estate copy for inheritance, court decisions for divorce settlements, Sale

contracts for property or investment sales, Latest payslip or Employment contract for employment)

Refer to AML Guidance on establishing Source of Funds (SOF) and Source of Wealth (SOW) issued by ICPAC, for further details.

Other documents

Professional Reference Letter	Reference Letter from a professional Lawyer or Accountant within the EEA.

Legal Entities

The following is a suggested non-exhaustive list of sources of evidence:

Type of Information	**Source of Verification**
Incorporation Name, Date & Number	Certified true copies of the statutory documents confirming the Incorporation date and number (e.g. for Cyprus Companies Certificate of Incorporation)
Registered Office*	Certified true copies of the statutory documents confirming the registered office (e.g. for Cyprus Companies Certificate of Registered Office)
Board of Directors	Certified true copies of the statutory documents confirming the Board of Directors (e.g. for Cyprus Companies Certificate of Directors and Secretary)
Current Shareholders	Certified true copies of the statutory documents confirming the current shareholders (e.g. for Cyprus Companies Certificate of Shareholders)
Governing Document	Certified true copies of the statutory governing documents of the entity (e.g. for Cyprus Companies Memorandum and Articles of Association)
Certificate of Good standing	Evidence supporting that the entity is in a Good Standing (e.g. for Cyprus Companies certified true copy of the certificate of Good Standing – applicable for companies with more than 6 months of existence)
Financial and other Information (where applicable)	Group structure and the Latest Financial Information reports (e.g. for Cyprus Companies Latest Audited Financial Statements)

***** *In addition to the registered address, actual business address shall be obtained.*

The above documents can be printed by the website of the Registrar of Companies and must be annotated. It is highlighted, that firms should not rely ~~independently~~ solely on the Beneficial Owner Directory for their identification and due diligence obligations.

Legal Arrangements (Trust, foundations and other similar legal arrangements)

Type of Information	**Source of Verification**
Name, Date & Number	Certified true copies of the documents confirming the registration date and number (e.g. Proof of registration with the relevant supervisory authority)
Governing document	Certified true copies of the trust deed and any subsequent and/ or additional amendments
Trustee/Settlor/Protector /Beneficiaries/other person exercising control over the legal arrangement (including fund managers, accountants, tax officials (if applicable))	Certified true copies Trust deed and any subsequent deeds of appointment or retirement and Certified true copies of the documents outlined above for natural and legal persons, depending on the nature of each person (e.g see above details for natural or legal persons)
Trust assets	Certified true copies of the trust deed and any subsequent and/ or additional amendments. Depending on the source of wealth or source of funds of the trusts, relevant and sufficient documentary evidence must be obtained (e.g., financial statements, tax assessment, sale purchase agreements, grant of probate etc)
Nature and activity of the trust	Certified true copies of the trust deed and any subsequent and/ or additional amendments.

Listed Entity

Type of Information	Source of Verification
Full name	Annotated printout from the web-site of the relevant body
Registered Address	The printout should contain its registered address
Membership or registration number	The printout should contain its registered number

Certification

The following is a suggested non-exhaustive list of methods of certification:

a) A Notary Public – (not Certifying Officer)
b) Apostille (Hague Convention) – Legalisation of Public Documents for Compatible countries
c) The Embassy or Consulate of the Cyprus Republic

The certification must indicate that the document is a “Certified true copy of the original”, state the certifier’s name, capacity and the date of certification.

ANNEX IV – Money Laundering red flags

Examples of suspicious transactions/ activities related to money laundering:

1. Transfer of funds between bank accounts established in various countries, through Cyprus, without justified reason.
2. Transfer of funds between companies belonging to the same group, without justified reason.
3. Deposits performed without submission of supporting documentation in an accepted form (e.g. invoice, agreements etc.).
4. Supporting documentation that is submitted in relation to a specific transaction (e.g. an invoice or agreement) is not in the same form that is normally used by the client. For example draft invoices, different from those produced from the system used by the client are submitted.
5. Transactions with no apparent purpose or which are unnecessarily complex.
6. Use of foreign bank accounts or companies or groups of companies with a complicated ownership structure which is not justified based on the needs and economic profile of the client.
7. The transactions or the size of the transactions requested by the client do not comply with the client's usual practice or business activity.
8. Large volume of transactions and/or money deposited or credited into an account, when the nature of the client's business activities would not appear to justify such activity.
9. Frequent settlement of client's obligations in cash.
10. Use of bank accounts other than the client's usual bank accounts, to transfer amounts initially deposited in cash.
11. Any transaction of which the nature, size or frequency appears to be unusual.
12. Instructions of payment to a third person that does not seem to be related with the instructor.
13. Transfer of funds to and from countries or geographical areas which do not apply or inadequately apply the FATF Recommendations.
14. A client is reluctant to provide complete information when establishing a business relationship about the nature and purpose of the client's business activities, anticipated account activity, names of officers and directors, or business location.
15. A client is providing minimum or misleading information that is difficult or expensive for the firm to verify.
16. A client provides unusual or suspicious identification documents.
17. A client's home/business telephone is disconnected and the client cannot be reached by the firm and its employees.

18. A client who has been introduced by a foreign financial organisation, or by a third party from countries or geographical areas which do not apply or inadequately apply the FATF Recommendations.
19. Financial transactions from non-profit or charitable organisations for which there appears to be no logical economic purpose or for which there appears to be no link between the stated activity of the organisation and the other parties in the transaction.
20. Unexplained inconsistencies arising during the process of identifying and verifying the client.
21. Complex trust or nominee network and/or legal structure.

ANNEX V – Terrorist Financing red flags

Examples of suspicious transactions/activities related to terrorist financing:

1. A series of complicated transfers of funds from one legal or physical person to another as a means to hide the source and intended use of the funds.
2. Transactions which are inconsistent and are not economically justified considering the organisation's normal activity.
3. Deposits are structured below the reporting requirements to avoid detection.
4. Multiple cash deposits and withdrawals with suspicious references.
5. Frequent domestic and international ATM activity.
6. Funds transfers do not include information on the originator, or the person on whose behalf the transaction is conducted, when the inclusion of such information would be expected.
7. Unusual cash activity in foreign bank accounts.
8. Multiple cash deposits in small amounts in an account followed by a large wire transfer to another country.
9. Use of multiple, foreign bank accounts.
10. Multiple personal and business accounts or the accounts of non-profit organisations or charities are used to collect and funnel funds to a small number of foreign beneficiaries.
11. Foreign exchange transactions are performed on behalf of a customer by a third party, followed by funds transfers to locations having no apparent business connection with the customer or to higher-risk countries.
12. Transactions involving foreign currency exchanges are followed within a short time by funds transfers to higher-risk locations.
13. Multiple accounts are used to collect and funnel funds to a small number of foreign beneficiaries, both persons and businesses, particularly in higher-risk locations.
14. Wire transfers to areas of conflict.
15. Financial activity identifiable with travel (e.g. purchase of airline tickets) to jurisdictions adjacent to areas of conflict.
16. Sudden conversion of financial assets to a virtual currency exchange or virtual currency intermediary that allows for increased anonymity.
17. The parties involved in transactions (owner, beneficiary, etc.) are from countries known to support terrorist activities and organisations.
18. Use of false corporations, including shell-companies.
19. Existence of media reports referring to account holder who are linked to known terrorist organisations or is engaged in terrorist activities.