ABALONE ASSET MANAGEMENT LTD

ANTI MONEY LAUNDERING AND
COUNTER FUNDING OF TERRORISM MANUAL
(the 'Manual')

2018

Document History

Version	Date	Author/Editor	Changes/Modifications	Status
1.0	1st August 2015	Tonio Fenech	Final	Approved
2.0	1st August 2016	Riccardo Teodori	Final	Approved
3.0	15st March 2017	Carmine Reho	Final	Approved
4.0	31st March 2018	Carmine Reho	Final	Approved

This policy applies from 1st August 2015 and has been approved by the board of directors (the "*Board*").

TABLE OF CONTENTS

ABBREVIATIONS 7

PREFACE..... 8

1. The Policy 9

Obligations of Abalone Asset Management Limited, its Directors and Employees 10

2. Local and International Legislative Frameworks 10

2.1. Local Legislative Framework 10

The Prevention of Money Laundering Act (PMLA) and the Prevention of Money Laundering and Funding of Terrorism Regulations (PMLFTR) 11

The Financial Intelligence Analysis Unit (FIAU) and Implementing Procedures 12

2.2. International Framework 12

Financial Action Task Force (FATF) 12

Council of Europe 12

3. Customer Due Diligence (CDD) 13

3.1. The Identification and Verification Process 13

Language used 19

3.2. Information on the purpose and intended nature of the business relationship . 19

3.3. Timing of CDD 19

3.4. Ultimate Beneficial Owner (UBO) 19

Agent – Principal Relationship..... 20

Other Minority Shareholders 21

3.5. Reputable Jurisdictions 21

3.6. On-going Monitoring 22

3.7. Source of Funds and Wealth..... 22

Method of Payment Used 23

Evidence of source of funds 23

Funds received from High Risk Countries 23

4. Risk-based Approach and Customer Acceptance Policy and Procedure 23

4.1. Simplified Customer Due Diligence (SCDD) 24

4.2. Enhanced Customer Due Diligence (ECDD)..... 25

4.3. Non face-to-face relationship 25

4.4. Politically Exposed Persons (PEPs) 25

4.5. Risk Based Approach (RBA) 26

On-going updating of the client profile (re-classification): There might be situations where the client is classified as low in terms of money laundering and financial of terrorism risk but his risk profile changed to high due to his personal circumstances. For example a client becomes a PEP. In such event the name of the client shall be referred to the MLRO and board for reviewing and approval..... 30

4.6. Reliance on Third Parties or other Subject Persons 30

4.7. Customer Acceptance Policy 31

4.8. General Prohibitions 32

5. Vetting of Employees and Training Requirements 32

5.1. Due Diligence on Employees 32

5.2. Employee Training 32

6. Record Keeping and Access to Clients' Files 33

6.1. Record Keeping Time-frames..... 33

7. MLRO and the Reporting of Suspicious Transactions 34

7.1. The Money Laundering Reporting Officer 35

7.2. Police Investigations and Court Orders 36

7.3. Reporting Suspicious Activity and Transactions 36

7.4. Procedures for filing a Suspicious Transaction Report 36

7.5. Confidentiality and Tipping Off 37

7.6. Record Keeping of STRs 37

7.8. Annual Compliance Report 37

APPENDICES SECTION 39

ABBREVIATIONS

9/11	**Terrorism attacks of the 11th September 2001**
AML	**Anti-money laundering**
CDD	**Customer Due Diligence**
ECDD	**Enhanced Customer Due Diligence**
EU	**European Union**
FATF	**Financial Action Task Force**
FIAU	**Financial Intelligence Analysis Unit**
FT	**Funding of Terrorism**
MFSA	**Malta Financial Services Authority**
ML	**Money Laundering**
MLRO	**Money Laundering Reporting Officer**
NCCT	**Non-Cooperative Countries or Territories**
PEP	**Politically Exposed Person**
PMLA	**Prevention of Money Laundering Act**
PMLFTR	**Prevention of Money Laundering and Funding of Terrorism Regulation**
RBA	**Risk Based Approach**
SCDD	**Simplified Customer Due Diligence**
STR	**Suspicious Transaction Report**
UBO	**Ultimate Beneficial Owner**
UN	**United Nations**

PREFACE

These policies and procedures have been approved by the Board of Directors and came into force as of the 1st August 2015. These policies and procedures are subject to annual review. These policies should also be reviewed in the light of industry developments, in an effort to maintain the Company's best practice policy.

The objective of this document is to establish and maintain policies, procedures and controls which deter criminals from using the Company's facilities for money laundering and the funding of terrorism

These policies and procedures are subordinate to the PMLA, PMLFTR and the Implementing Procedures referred to below, and the Company, its officers and employees must always refer directly to the PMLA, PMLFTR and the Implementing Procedures when ascertaining and implementing its AML obligations in terms of law.

This document is for internal use only and should not be circulated outside of Abalone Asset Management Ltd.

1. The Policy

1. The anti-money laundering ("AML") and counter-funding of terrorism ("CFT") obligations of Abalone Asset Management Ltd (the "Company"), acting through its Directors, officers and managers, are set out under the:

   i. Prevention of Money Laundering Act, 1994 as amended (Chapter 373, the laws of Malta) (the "**PMLA**");
   ii. Prevention of Money Laundering and Funding of Terrorism Regulations, 2008 (Subsidiary Legislation 373.01) (the "**PMLFTR**");
   iii. The Criminal Code (Chapter 9, the Laws of Malta); and
   iv. Implementing Procedures Part I, issued by the Financial Intelligence Analysis Unit, 20th May 2011 as amended.

2. The term 'money laundering' is generally described as the process by which the illegal nature of criminal proceeds is concealed or disguised in order to lend a legitimate appearance to such proceeds. Furthermore, money laundering also takes place when a person knowingly facilitates the untruthful justification of the origin of an asset (nature, location, movement, ownership), and assists in disguising, transferring, or converting proceeds of crime. The methods by which money may be laundered are varied and can range in sophistication.

3. Whatever method is used to launder money, the process is normally accomplished in three stages:

Placement Stage	The money originating through an illegal activity is integrated into the financial system. The money is placed into different bank accounts, or investments usually in small amounts;
Layering Stage	A series of transfers between various bank accounts is undertaken, with the objective of distancing them from the source (i.e. the illegal activity);
Integration Stage	The money is used for the purchase of assets (such as financial investments or real estate) or in the investment of legitimate businesses. This is done in order to legitimise the money originating from an illegal activity.

4. The Criminal Code addresses, amongst other matters, acts of terrorism, terrorist groups, terrorist property and funding of terrorism.

5. **Terrorist financing** is the act of providing funds for terrorist activity. It may involve funds raised from legitimate sources, such as personal donations and profits from businesses and charitable organizations, as well as from criminal sources, such as drug trade, human and weapon smuggling, fraud, kidnapping and extortion.

6. Terrorists use techniques like those of money launderers to evade authorities' attention and to protect the identity of their sponsors and of the ultimate beneficiaries of the funds. When terrorists raise funds from legitimate sources, the detection and tracking of these funds becomes more difficult. After the 9/11 events Counter Financing of Terrorism legislation (CFT) was included as part of the anti-money laundering legislative structure.

7. The proliferation of worldwide illegal activities and economic globalisation has placed the risks of money laundering and terrorist financing at the forefront of the agenda of the world's leading financial jurisdictions. The risk of having businesses or assets being financed through illegal activities is a reality which needs to be

appropriately addressed. To this end, reputable jurisdictions, including Malta, have put in place a legislative framework and guidelines for addressing this issue and to devise the necessary controls to ensure that such occurrences are both prevented and detected at an early stage.

Obligations of Abalone Asset Management Limited, its Directors and Employees

8. Abalone Asset Management Limited, hereafter called the 'Company', holds a Category 2 license issued by the MFSA in terms of the Investment Services Act (Chapter 370 of the Laws of Malta). The Company's investment services license falls under the definition of relevant financial business[1] in terms of the Prevention of Money Laundering and Funding of Terrorism Regulations (PMLFTR) and is therefore subject to such legal requirements. In terms of its licence, the Company is authorised to provide investment management services to Alternative Investment Funds ("AIFs") and UCITS Schemes ("UCITS").

9. Non-compliance with the AML/CFT legislation and FIAU's Implementing Measures could expose the Company to financial and criminal sanctions, regulatory risk and a reputational damage to its corporate brand image. The maximum penalties and offences presented hereunder may also be imposed by the relative Competent Authorities.

   - PMLA offences: a penalty not exceeding EUR2,500,000 and/or imprisonment for a term not exceeding 18 years; and

   - PMLFTR infringements: Penalty ranging from EUR1,000 to EUR 50,000 may be inflicted on the Company where an offence against the provisions of these regulations is committed. Other repercussions include 'Name and Shame' in terms of which infringements or breaches in terms of the PMLFTR are published on the MFSA website.

10. The Company's directors and employees are required to comply with the guidelines and procedures detailed in this Manual and to exercise care when applying due diligence during the course of their work.

11. In order to meet the Company's high ethical standards and to mitigate the aforementioned compliance risks, the company is obliged to;

    i) identify the requirements for the prevention of money laundering and funding of terrorism;
    ii) define the procedures that need to be followed in order to mitigate money laundering and terrorist financing risk which the Company can face during the course of its business which takes into account a risk-based approach in line with market practice;
    iii) explain the due diligence process that needs to be undertaken in satisfaction of the requirements of relative legislation and FIAU expectations; and
    iv) outline the process for reporting suspicious transactions identified.

2. Local and International Legislative Frameworks

2.1. Local Legislative Framework

[1] Please refer to Appendix 1 to these Procedures.

The Prevention of Money Laundering Act (PMLA) and the Prevention of Money Laundering and Funding of Terrorism Regulations (PMLFTR)

12. The anti-money laundering regime is based on two main pieces of legislation, namely the Prevention of Money Laundering Act (Chapter 373 of the Laws of Malta) and the Prevention of Money Laundering and Funding of Terrorism Regulations (Subsidiary Legislation 373.01). Since 1994, the Regulations were subject to various amendments which reflect the corresponding international and European developments. In fact the PMLFTR transpose the Third Anti-Money Laundering Directive (Directive 2005/60/EC) which, in turn, is modelled on the FATF 40 Recommendations and 9 Special Recommendations (further revised on the 15th February 2012) which became the global standard for anti-money laundering ("AML") and combating the financing of terrorism ("CFT"). The Fourth Money Laundering Directive was published on the 5th June 2015. This comes with revamped regulation on information to be provided to the subject person on the transfer of funds. The transposition deadline is the 26th June 2017.

13. The PMLA establishes the foundations for the legal AML framework, the investigative and prosecution powers for anti-money laundering offences and the establishment of the FIAU.

14. The PMLA also defines money laundering as:

    i) the **conversion or transfer of property** knowing or suspecting that such property is derived directly or indirectly from or the proceeds of, a criminal activity or from participation is such criminal activity for the purpose of or purposes of concealing or disguising the origin of the property or of assisting any persons involved or concerned in criminal activity;
    ii) the concealment **or disguise of the true nature, source, location, disposition, movement, rights** with respect of, in or over, or ownership of property, knowing or suspecting that property is derived directly or indirectly from a criminal activity;
    iii) the **acquisition, possession or use of the property** knowing or suspecting that the same was derived or originated directly or indirectly from criminal activity or through participation in criminal activity;
    iv) **retention without reasonable excuse of property** knowing or suspecting that the same was derived or originated directly or indirectly from criminal activity or from an act or acts of participation in criminal activity;
    v) **attempting any of the matters or activities above**; or
    vi) **acting as an accomplice** in respect the above activities.

15. The term 'criminal activity' includes any activity which is considered as a crime in terms of the Criminal Code.

16. It is worth noting that terrorist financing is defined under Article 328F of the Criminal Code. Under the above-mentioned article, 'funding of terrorism' is the process by which terrorist organisations or individual terrorists are funded in order to be able to carry out acts of terrorism. The term 'process' is defined as the process by which a person 'receives, provides or invites another person to provide, money or other property intending it to be used, or which he has reasonable cause to suspect that it may be used, for the purposes of terrorism'. The PMLFTR list out the definitions and obligations that subject persons are required to fulfil and to implement, in respect of:

    - Customer Due Diligence;
    - Customer acceptance procedures and risk-based approach;
    - Record Keeping;
    - Reporting of suspicious transactions and reporting to the FIAU;

- Initial and on-going AML/CFT training of employees;
- Compliance Management and Communication; and
- Due diligence on employees

17. The above listed requirements are in turn reflected in the FIAU Implementing Procedures and are reflected in this Manual to the extent applicable.

The Financial Intelligence Analysis Unit (FIAU) and Implementing Procedures

18. The FIAU was set up in 2001 by virtue of Act XXXI of 2001, through the inclusion in the PMLA of a number of provisions which provide for the establishment of the FIAU and defines its powers and functions. The FIAU is a government agency having a distinct legal personality which is responsible for the implementation of the AML/CFT regime in Malta. The FIAU issued the 'Implementing Procedures – Issued by the Financial Intelligence Analysis Unit in terms of the Provisions of the Prevention of Money Laundering and Funding of Terrorism Regulations – Part I', referred to as the Implementing Procedures. The purpose of the Implementing Procedures is to assist subject persons in understanding and fulfilling their obligations under the PMLFTR, thus ensuring an effective implementation of the provisions of the PMLFTR. Suspicious transaction reports (which will be covered in section 7 of these procedures) are to be forwarded to the FIAU. The FIAU is also responsible for the collection, collation and analysis of suspicious transactions reports received from subject persons.

2.2. International Framework

Financial Action Task Force (FATF)

19. FATF was set up in response to mounting concern over money laundering, and recognition of the threat posed to the financial system. The initial brief for the FATF was to examine money laundering techniques and trends, reviewing the action which had already been taken at a national or international level, and setting out the measures that still needed to be taken to combat money laundering.

20. The FATF issues recommendations which are recognised as global AML and CFT standards. In 1990, the FATF issued the first 40 AML recommendations which were subsequently revised in 1996 and 2003. Following the events of 9/11, the FATF issued 9 special recommendations on Terrorist Financing. In February 2012 the FATF issued revised standards. The new standards strengthen the requirements for higher risk situations and allowed countries to take a more focused approach in areas where high risks remain or implementation could be enhanced.

21. As part of its missions, the FATF monitors members' progress in the implementation of AML / CFT measures. As a result of this assignment, the FATF is able to identify countries and jurisdictions that fall under the definition of high-risk and non co-operative jurisdictions for the purpose of money laundering and funding of terrorism.

Council of Europe

22. On 8 November 1990, the Strasbourg Convention on Money Laundering, Search, Seizure and the Confiscation of proceeds from crime was signed, with the first EU Directive of the 19 June 1991, followed by the Second EU Directive of the 4 December 2001 as amended by the Third AML Directive. Another important directive worth noting is EU Directive 2006/70/EC of the 1st August 2006, which deals with the definition of politically exposed persons (PEP) and technical criteria for simplified due diligence. EU Directive 2015/849 of the European Parliament and of Council of the 20th May 2015 was published on the 5th June 2015 and repeals the

Third AML Directive. Its transposition deadline is the 26th June 2017. The provisions of this Directive have not yet been implemented in local legislation.

23. The UN is the main world organisation to have delved in the issue of money laundering and funding of terrorism and its prevention. The UN is competent to adopt legally binding treaties and international agreements, and has throughout the years secured various conventions which addressed the prevention of money laundering, such as the adoption of the Vienna Convention (Illicit Traffic in Narcotic Drugs and Psychotropic Substances) in 1988 and the Palermo Convention of 2003 (designed to harmonise penal sanctions and recommends improved judicial cooperation) amongst others.

3. Customer Due Diligence (CDD)

24. CDD is the process by which the identity of an applicant for business is identified and verified; the identification and verification of ultimate beneficial ownership in case of a body corporate, trust and similar legal arrangements; the establishment of the purpose and intended nature of the business relationship and ongoing monitoring. The concept of CDD does not relate to the applicant for business only but it extends to all persons with whom the Company has established a business relationship including employees.

25. As a subject person, the Company is responsible to carry out CDD processes and is required to perform such due diligence checks and to comply with the requirements set out in applicable law and described hereunder. As part of this process, the Company should establish the risk profile of the client on risk indicators as described in terms of Table 6 of this Manual.

26. In respect of Clients or applicants for business classified as higher risk in terms of money laundering and funding of terrorism, may only be accepted if approved by two board members.

3.1. The Identification and Verification Process

27. The identification and verification of the identity of an applicant for business needs to be carried out on the basis of documents, data or information obtained from a reliable and independent source. The below describes how identification and verification of clients has to be carried out in line with the applicable FIAU Implementing Procedures.

Table 1 – Basic CDD Requirements

Identification	Identification takes place by obtaining the person's details and other relevant information in relation to that person. The information obtained on natural persons (individual) and legal persons (such as in the case of companies, partnerships, trusts etc.) would vary accordingly. Information which must be collected in respect of each type of person is described below: *Individual/Natural Person* a) Official full name; b) Place and date of birth; c) Permanent residential address; d) Identity reference number, where available; and e) Nationality. *Legal Person: Limited Liability Company (Private and Public) /Partnership / Foundation* a) Official full name of legal person; b) Registration number (this might not be applicable or available for foundations); c) Date of incorporation or registration; and d) Registered address or principal place of business (in case of companies and partnerships). *Trust* a) Official full name of the trust; b) The nature and purpose of the trust; and c) Country of establishment. It is a requirement that the ultimate beneficial owner particularly in case of legal persons is verified and identified. The definition of beneficial owner is detailed under Table 3 and Appendix 2.

Verification	Verification takes place by making reference to documents, data or information obtained from the applicant for business. In order for verification to be completed in line with the PMLFTR, the documents obtained from clients need to satisfy the following criteria: a) They have to be reliable; and b) Issued from an independent source, such as a government authority, department or agency; a regulated utility company such as telephone companies, water and electricity providers or a subject person carrying out relevant financial business (as defined in terms of Appendix 1 to these Procedures) in Malta, in a Member State of the EU or in a reputable jurisdiction. A utility company is an organization that maintains the infrastructure for the provision of a public service. Utility services incorporate electricity, natural gas, water and sewage. Bills presented by an applicant for business and which relate to the provision of any of the above services are acceptable as part of the customer due diligence process. All documentation received has to be certified. Certifications are to be undertaken by an official of the Company or by an introducer (as described above). The certification has to be evidenced by a written statement confirming the following: In case of *Proof of Address* the following should be stated: *The document has been seen and verified by the certifier and it is a true copy of the original document.* In the case of *Proof Of Identity* the following should be stated: *The photo is a true likeness of the applicant for business/ the beneficial owner (as the case may be) and it is a true copy of the original document.* The contact details and designation of the certifier have to be included together with the date when certification has been carried out.

The below table (Table 2) outlines the documentation that should be obtained as part of the verification of identity both in relation to an individual/natural personal or a corporate/legal entity.

Table 2 - CDD Documentation

1.0 Individuals	Identification Documents, which contains a photographic image of the applicant for business: • **Valid and unexpired** National ID card / Passport / Driving licence Proof of address (any one of the below): • Bank statement issued by a credit institution licensed in a reputable jurisdiction (refer to table 4); or • Utility bill issued either by a fixed telephone company, electricity, water or gas supplier company. Mobile phone statement are not acceptable for CDD purposes; or • Correspondence from a central or local government authority, department or agency confirming address; • Any government issued document listed above, where a clear indication of the residential address is provided. In case of a utility bill, bank statement or statement issued by a relevant financial business, the issue date must not be older than six (6) months. The name of the applicant for business needs to be checked against sanction lists.

2.0 Legal Entities (Private/Public Companies, and Partnerships)	• The following documentation has to be obtained from clients who are legal persons: • Notarised (or certified by the relevant company registrar, company secretary or director, or a legal professional, accounting professional, a person undertaking relevant financial business or a person undertaking an activity equivalent to relevant financial business in another jurisdiction) copy of or original Certificate of Incorporation and any Change of Name Certificate; and/or • Notarised (or certified by the relevant company registrar, company secretary or director or a legal professional, accounting professional, a person undertaking relevant financial business or a person undertaking an activity equivalent to relevant financial business in another jurisdiction) copy of, or original Memorandum and Articles of Association, partnership agreement (in the case of a Partnership) or other constitutive document in the case of a Foundation; and/or • Registry search confirming that the company or partnership has not been or is not in the process of being wound-up, struck-off or terminated. Where this information is not available, a certificate of incumbency or certificate of good standing shall be obtained instead; and • A list, identifying all directors and partners (in the case of a Partnership) where the official full name, permanent residential address, place and date of birth, nationality and identification number is obtained (no verification is required); and • Identification information on the ultimate beneficial owners (official full name, permanent residential address, place and date of birth, nationality and identification number) and verification of the same as per 1.0 above (identification document and proof of address); and • Organisational Chart and explanation of ownership; and • Identification information and verification documentation of the directors, ultimate beneficial owners and all persons included on the organisational chart (check against sanction lists and PEP lists)

3.0 Trusts	The following documentation should be obtained from clients that qualify as a trust: • Notarised (or certified as mentioned above) copy of, or original Trust Deeds; and • Identification of the beneficiaries, settlor, custodian and protector, if any, (official full name, permanent residential address, place and date of birth, nationality and identification number should be obtained as applicable) and verification documentation as per 1.0 above in case of natural persons (identification documents and proof of address) and 2.0 above in case of a corporate entity; and • Identification information and verification documentation on the Trustee as per 1.0 above (official full name, permanent residential address, place and date of birth, nationality and identification number, and identification documents and proof of address); and • Copy of the authorisation of the trustee issued by the relevant authority for that person to act as trustee.
4 . 0 Foundations	The following documentation has to be obtained from clients set up as Foundations: • Notarised (or certified by one of the founders or associates, a lawyer, accountant, notary, or a person undertaking relevant financial business or equivalent activity) copy of or original Certificate of Registration and any Change of Name Certificate; and/or • Notarised (or certified by one of the founders or associates, a lawyer, accountant, notary, or a person undertaking relevant financial business or equivalent activity) copy of, or original constitutive document; and • A list identifying persons vested with the representation and administration of the foundation as well as the class of persons in whose interest the foundation was set up and the founder and/or any other person (other than the founder) who has endowed the foundation and any person who has been assigned any rights previously pertaining to the founder (official full name, permanent residential address, place and date of birth, nationality and identification number should be obtained); and • Organisational Chart and explanation of ownership; and • Identification information and verification documentation of the founder or associates, persons other than the founder who have endowed the Foundation and persons in whose interest the Foundation has been set up (check against sanction lists and PEP lists).

Language used

28. All client documentation must be translated into the English language, dated and signed by the person who has carried out the translation.

29. Where the documentation is received in a language not understood by the Company, translation from a professional translation company shall be obtained. The translation should be dated, signed and certified by an independent person of proven competence confirming that it is a faithful translation of the original.

3.2. Information on the purpose and intended nature of the business relationship

30. Once the identification and verification of the applicant for business has been carried out, the Company has to obtain information on the purpose and intended nature of the business relationship in order to be in a position to establish the business and risk profile of the applicant for business. This obligation does not apply when the applicant for business only seeks to carry out occasional transactions.

3.3. Timing of CDD

31. The timing of CDD is critical. Delays in completion of the above CDD process may expose the Company to money laundering and funding of terrorism risk. At the same time, CDD completion may not always be realistic and reasonable. In line with the FIAU Implementing procedures, it is imperative that the identification stage and inter alia CDD documentation requirements, as aforementioned, are duly applied to all prospective clients or applicants for business who take active steps to establish a business relationship. On the other hand, it would be premature for the Company to request CDD documentation at a preliminary business meeting or where the applicants calls in for information. In the case of the Company the process of CDD is initiated where the Client or applicant of business has communicated of his intension to appoint the Company as its service provider.

3.4. Ultimate Beneficial Owner (UBO)

32. As mentioned above, it should be noted that customer due diligence checks must go beyond the direct customer or contact person. There might be situations where the customer is acting as a front person for other persons (both natural and legal persons). Therefore due diligence must be extended to the UBO/s in whose name or in whose account the direct customer is acting. The identification and verification requirement also apply for situations where the person is representing another person; or in the context of legal persons ultimate shareholders / founders / beneficiations / partners. Beneficial owners that would be subject to due diligence would be those that fall under one of the below situations (Table 3):

Table 3 - Persons qualifying as beneficial owners

	TYPE	DEFINITION

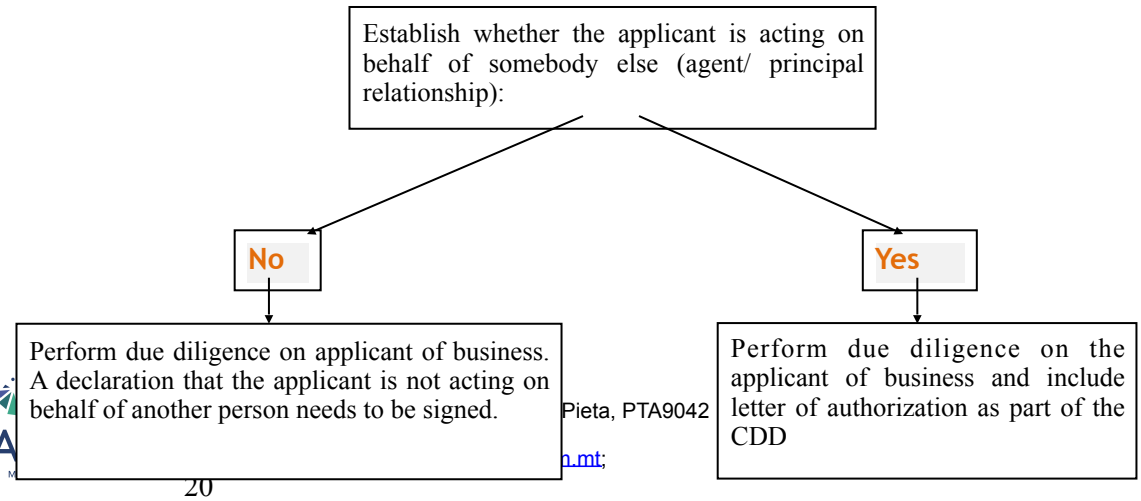
A.	**Body corporate or body of persons**	(i) A natural person/s that has: • Direct ownership of more than 25% (including bearer shares); or • Direct ownership of more than 25% voting rights; or • Direct control of more than 25% (including bearer shares); or • Direct control of more than 25% voting rights; or • Indirect ownership of more than 25% shares (including bearer shares); or • Indirect ownership of more than 25% voting rights; or • Indirect control of more than 25% shares (including bearer shares); or • Indirect control of more than 25% voting rights. (ii) A natural person who otherwise exercises control over the management of that body corporate or body of persons.
B.	**Legal entity or legal arrangement which administers and distributes funds**	(i) Determined beneficiaries – natural persons who are the beneficiaries of at least 25% of the property; (ii) Non determined beneficiaries – the class of persons in whose main interest the legal entity or arrangement is set up or operates; (iii) A natural person who controls at least 25% of the property of the legal entity or arrangements.

Appendix 2 provides examples of who should fall under the definition of beneficial owners in line with the PMLFTR.

Agent – Principal Relationship

33. There might be situations where the applicant for business or client is acting as an agent on behalf of another person (referred to as the principal). In such circumstances, both the agent and the principal are subject to CDD. In addition the agent needs to present a declaration from the principal authorizing him/her to act on his or her behalf. This could include a board resolution authorizing such persons to act on behalf of the Company. A Power of Attorney, a Management Agreement and/ or Fiduciary Agreement from the principal attesting that the agent can act on behalf of the principal are also acceptable documents. In the event that the applicant for business qualifies for the application of simplified due diligence, then such additional measures need not be applied.

34. The following process flow has to be followed in order to assess whether a person is acting on behalf of a principal:



Other Minority Shareholders

35. All persons (both natural and legal persons) who own a stake in the legal entity or have a direct or indirect shareholding even if these do not need to be subject to due diligence as per above, need to be checked on online databases which incorporate United Nations and the European Union sanctions. Should a match with such lists be encountered, the names and details are to be referred to the Money Laundering Reporting Officer (MLRO) and Compliance Officer for appropriate action.

3.5. Reputable Jurisdictions

36. PMLFTR makes reference to the term 'reputable jurisdictions'. Subject persons situated in the EU or in another reputable jurisdiction are subject to similar legislative measures and requirements for AML and CFT. Accordingly, the Company should be able to place a higher degree of reliance during its due diligence process.

37. Table 4 shows a list of all EU Member States and those other countries which have been recognised as having AML legislation which is equivalent to legislation in European Member States. In both cases, they are recognised as 'reputable jurisdictions' in terms of the PMLFTR. The Company shall keep the table updated rely on the below table when assessing the country risk of the applicant of business. Clients and applicants for business originating from the countries mentioned shall be classified as low risk and considered as residing in a reputable jurisdiction. Clients residing in countries not listed in the table below shall be assessed on the basis of Moneyval and FATF reports issued. In such situations, staff shall contact the Money Laundering Reporting Officer (MLRO) and Compliance Officer accordingly. The MLRO and Compliance Officer shall draw a country report on such country and present recommendation on the risk profile to be applied and the due diligence process to be followed for the approval of the board. The final decision of the board shall be presented to the staff and this Manual shall be updated accordingly to reflect the stance of the Company in this regard.

38. The Company shall also inform the FIAU of transactions and/or business relationships with persons, companies or undertakings, including those carrying out relevant financial business or a relevant activity from a non-reputable jurisdiction, which continue not to apply measures equivalent to those laid down in the PMLFTR (Category 1 non-cooperative jurisdictions as mentioned in the FATF Public Statement as referred to in Appendix 3 of this Manual). In such circumstances the FIAU, in collaboration with the relevant supervisory authority, may require that the Company terminates the business relationship or does not carry out the transaction. It may also impose appropriate counter measures deemed necessary in the circumstances.

Table 4 - List of Reputable Jurisdictions

EU Countries and EEA Countries **EEA Countries**	Austria; Belgium; Bulgaria; Cyprus*; Czech Republic; Denmark; Estonia; Finland; France; Germany; Greece; Hungary; Ireland; Italy; Latvia; Lithuania; Luxembourg; Malta; Netherlands; Poland; Portugal; Romania; Slovakia; Slovenia; Spain; Sweden; United Kingdom; Croatia Iceland, Norway, Liechtenstein. *It should be noted that Cyprus has been earmarked on the high alert by the Financial Intelligence Analysis Unit due to its associations with Russia.
Countries which have been recognised as having third country equivalence	Australia; Brazil; Canada, Hong Kong; India; Japan; South Korea; Mexico; Singapore; Switzerland; South Africa; The United States of America. French Overseas Territories such as (Mayotte, New Caledonia, French Polynesia, Saint Pierre and Miquelon and Wallis and Futuna) and Aruba, Curacao, Sint Maarten, Bonaire, Sint Eustatius and Saba, are included. The UK Crown Dependencies such as (Jersey, Guernsey, and Isle of Man) are also considered as equivalent by the EU.

3.6. On-going Monitoring

39. Ongoing monitoring is essential to ensure that, once the CDD of a customer has been completed, any business deals or transactions that are unusual or irrational are analysed to ascertain if there is any money laundering or terrorist financing involved. Ongoing monitoring on the Company's customers should include:
    - The scrutiny of transactions undertaken throughout the course of the relationship to ensure that the transactions being undertaken are consistent with the subject person's knowledge of the customer, its business and risk profile, including where necessary, the source of funds which have been obtained at the outset of the business relationship; and
    - Ensuring that the documents, data or information held by the subject person are kept up to date. In this regard, new documentation shall be obtained where an ID card or passport have expired.

40. As part of ongoing monitoring, the Company's employees are to be vigilant for:

    - **Complex or large transactions that have no apparent economic or visible lawful purpose**;
    - **Unusual patterns of transactions that have no apparent economic or visible lawful purpose**;
    - **Transactions which are particularly likely, by their nature, to be related to ML/FT**. Under this notion, attention should be paid to names of clients which have been sanctioned or included on terrorists lists;
    - **Investments which do not tally with the profile and knowledge of the client in question**;
    - **Business relationships and transactions with persons from non-reputable jurisdictions.** Such jurisdictions are listed in Appendix 3;
    - **Early redemption requests made by the clients without a plausible reason;**

3.7. Source of Funds and Wealth

41. The Company is required to obtain information on the source of wealth and source of funds from the client. Both are important aspects within the due diligence process for the prevention of money laundering or funding of terrorism.

42. The source of funds is the activity, event, business, occupation or employment from which the funds used in a particular transaction are generated. On the other hand, source of wealth refers to the economic activity which generates the total net worth of the customer. Whereas the source of wealth is identified at the beginning of the business relationship and the information thereon is updated from time to time where new material developments arise in the course of the business relationship, the Company is required to identify the source of funds of individual transactions in accordance with the obligation of ongoing monitoring as set out above. The amounts of monies paid, origin of payment and the method of payment used have to be assessed with the profile and knowledge of the client.

Method of Payment Used

43. It should be noted that each method of payment and origin of funds can represent a varying degree of risk in terms of money laundering. In this regard, the method of payment can impact the level of due diligence (from standard to enhanced due diligence) at the creation of the business relation and during the course of the relationship. For example liquid cash is more synonymous with money laundering and therefore higher levels of due diligence should be applied. In the case of the Company, all money must originate from the bank account of the client held in its name. Third party payments are prohibited at all times.

Evidence of source of funds

44. Staff shall also request evidence of source of funds where the client falls under high risk category (see Table 6). This could be applied where the amounts of deposits are very high and where the money originates from non-reputable jurisdictions. The evidence obtained shall be consistent with the explanation provided by the client. The below are examples of evidence of source of funds that can be obtained from the client:

- Latest pay slips;
- Latest bank statements;
- Other evidence relating to inheritance or evidence of sale of assets etc…

Funds received from High Risk Countries

45. In addition to the above, the Company's employees should be particularly sensitive when funds are received from non-reputable jurisdictions and or from countries that are listed as primary money laundering risks in the US Department of State International Narcotics Control Strategy Report, or countries listed in the FATF non-cooperative countries. The names of countries mentioned in the above reports are listed under Appendix 3. Relative information from the client shall be requested together with evidence of source of funds as applicable.

4. Risk-based Approach and Customer Acceptance Policy and Procedure

46. Each client represents a different type of risk in terms of money laundering and the funding of terrorism. The level of due diligence carried out should be commensurate with the risk presented by the client. The rule of thumb is that higher risk clients or applicants for business are subject to a higher level of due diligence.

47. The risk-based approach is embedded in the PMLFTR. With this in mind, the above regulation provides for the situations where 'simplified customer due diligence' (SCDD) and 'enhanced customer due diligence' (ECDD), can be applied.

4.1. Simplified Customer Due Diligence (SCDD)

48. The PMLFTR considers situations where SCDD may be applied. In such circumstances, subject persons do not need to identify or verify the applicant for business or beneficial owner and need not carry out ongoing monitoring of that relationship. In case of the Company, SCDD can be applied for:

a) Entities which are authorised, licensed or regulated to undertake relevant financial businesses by the MFSA or another regulator located in an EU Member State or in a reputable jurisdiction (refer to Table 4 above); and
b) Legal persons listed on a regulated market and which are subject to public disclosure requirements. Such entities have to be listed on a regulated market which is licensed and regulated by the MFSA (such as in the case of the Malta Stock Exchange), or by a stock exchange located in a Member State or in a reputable jurisdiction (refer to Table 4 above); and
c) With respect to beneficial owners of pooled accounts held by persons carrying out a relevant activity under paragraph (c) of the definition of "relevant activity", as found in Appendix 1, domestically, from within the Community or from a reputable jurisdiction, provided that the Company shall ensure that supporting identification documentation is available, or may be made available, on request, to the institution that is acting as the depository for the pooled accounts; and
d) domestic public authorities or public bodies which fulfil all the following criteria:

    (i) The applicant for business has been entrusted with a public function pursuant to the Treaty on the European Union, the Treaties on the Communities or other Community legislation;
    (ii) The identification of the applicant for business is publicly available, transparent and verified;
    (iii) The applicant for business undertakes activities that are transparent, including any accounting practices; and
    (iv) The applicant for business is either accountable to a Community institution or to a domestic relevant authority or to an authority of another member of the Community or, where appropriate and effective procedures are in place to control the activity of the applicant.

49. It is important that in applying SCDD, the respective official regulators or regulated markets websites are consulted in establishing that the applicant for business falls in criteria set out above. Evidence of such should be included on clients' files. Where this is not possible, a certified true copy of the licence or authorisation by the relevant authority shall be requested in case of licensed entities.

50. During the above process, the MLRO shall be consulted for the relative approval for the use of SCDD. Moreover in case of suspicious activity or transactions identified, staff shall revert to normal due diligence or enhanced due diligence as applicable.

51. In the light of the above, where the Company provides investment services to regulated entities, such as UCITS schemes and / or Alternative Investment Funds (AIFs) regulated in the EU and EEA states, SDD measures may be applied on the understanding that the Companies clients, that is, the Funds, would be regulated in a European Member State. This would not apply in those circumstances where the Company manages AIFs which are not regulated in their home member state or other reputable jurisdictions, in which case, the rules on standard due diligence or enhanced due diligence would apply.

4.2. Enhanced Customer Due Diligence (ECDD)

52. The company must apply Enhanced Due Diligence in situations that represent a higher risk of money laundering or the financing of terrorism. The following circumstances are deemed to be situations that represent a higher risk:

    i. The client is not physically present for identification purposes (i.e. non-face to face business)
    ii. Business relationship or occasional transaction with a Politically Exposed Person ("PEP")

4.3. Non face-to-face relationship

In cases where the applicant for business cannot be physically present for identification purposes, the Company will not be in a position to establish that the person with whom it is transacting is actually the person he purports to be without resorting to additional measures to compensate for the higher risk. In such cases, the Company should apply **one or more** of the following measures;

(a) Establish the identity of the applicant for business by using additional documentation and information. Such documents containing identification details need to have been issued from the jurisdiction where s/he holds citizenship after producing an identification document containing a photograph.
(b) Verify or certify the documentation supplied using supplementary measures. The documentation should be verified by a legal professional, accountancy professional, a notary, a person undertaking relevant financial business or a person undertaking an activity equivalent to relevant financial business carried out in another jurisdiction.
(c) Require certified confirmation of the documentation supplied by a person carrying out relevant financial business.
Certification should be evidenced by a written statement saying that the document is a true copy of the original document, that the document has been seen and verified by the certifier and that the photo is a true likeness of the applicant for business or the beneficial owner.
(d) Ensure that the first payment or transaction into the account is carried out through an account held by the applicant for business in his name with a credit institution authorised under the Banking Act or otherwise authorised in another Member State of the Community or in a reputable jurisdiction.

4.4. Politically Exposed Persons (PEPs)

53. Politically exposed persons are individuals who hold prominent public positions/ offices. These would also include their family members and close associates. Where an individual has ceased to hold any of the offices mentioned in the definition of a PEP as described below for a period of at least 12 months, that person ceases to qualify as a PEP. Persons falling under this category are included in Table 5 below:

Table 5 - Definition of PEPs

PEPs	• Heads of State, Heads of Government, Ministers and Deputy and Assistant Ministers and Parliamentary Secretaries; • Members of Parliament; • Members of the courts or of other high-level judicial bodies whose decisions are not subject to further appeal, except in exceptional circumstances; • Members of the courts of auditors, audit committees or of the boards of central banks; • Ambassadors, charge d'affaires and other high ranking officers in the armed forces; • Members of the Ambassadors, charge d'affaires and other high ranking officers in the armed forces; • Members of the administration, management of boards of State-owned corporations.
The immediate family of a PEP	• The spouse or partner recognised by national law as equivalent to the spouse; • The children and their spouses or partners; and • The parents.
Close associates	• Individuals that have a joint ownership or a body corporate (e.g. company) or any other form of legal arrangement with the PEP; • Other close business relationships with that PEP; and • Individuals who have sole beneficial ownership of a body corporate or other legal form or legal arrangement that is known to have been established for the benefits of that PEP.

54. In the case where the Company has a business relationship with a PEP, the following enhanced CDD procedures should be undertaken:

- Advise the MLRO;
- Obtain senior management approval (approval from board of directors);
- Take adequate measures to establish the source of wealth and funds involved. In this regard, the Company shall obtain a statement from a relevant financial business confirming source of wealth and the evidence of source of funds; and
- Conduct enhanced ongoing monitoring.

55. The Company shall request information from the applicant for business as to whether he/she falls under the definition of a PEP as described above. PEP checks via Google or other data providers assist in identifying names of clients falling under PEP or related to a PEP.

4.5. Risk Based Approach (RBA)

56. In terms of the PMLFTR, the Company is expected to apply a risk based approach in relation to customer identification and transaction monitoring. This concept

essentially warrants a concentration of efforts on those clients assessed as being of a high risk, possibly in view of their country of origin, sector of operations, etc. Entities are required to have their procedures geared up to take into account the assessed level of money laundering/terrorist financing risk.

57. Money Laundering and Funding of Terrorism risks may be measured using various categories, which may be modified by risk variables.

58. The most commonly used risk criteria are:

    - Country risk;
    - Customer risk;
    - Services risk; and
    - Interface Risk.

59. The below Table 6 'Risk-based Approach Matrix' outlines the risk management framework to be applied by the Company in relation to money laundering and funding of terrorism risks on the basis of country risk, customer risk, services risk, and interface risk. The second row outlines the high extreme situations and which fall outside the risk appetite of the Company. The first column on the left specifies the level of due diligence that needs to be applied for the situations described under the relative risk co-ordinates.

Table 6 – Risk-based Approach Matrix

	Country Risk	Customer Risk	Services Risk	Interface Risk

Extreme	• Sanctioned countries (UN, EU) • Non-cooperative countries in AML matters (as identified by FATF and included under Appendix 3) • Countries providing funding/ support for terrorist activities (as identified by World Bank) • Countries having significant level of corruption and/ or criminal activity	• Sanctioned individuals/ entities • Arms manufacturers, dealers and intermediaries • Funds received from non-reputable jurisdictions or non-cooperative countries (As per Appendix 3). • Transactions utilising complex or opaque transactions. • PEPs from high risk countries. • Unregulated charities/not-for-profit organisations • Clients having bearer shares	• Dealing in Commodities of high risk (e.g. crude oil) • Bearer shares	• Non face-to-face business which is located in non-cooperative countries

High	• Other countries which fall outside the definition of reputable jurisdiction as per Table 4 and which are not listed under Appendix 3.	• PEPs • Cash intensive businesses or clients paying in cash • Dealers in high value and precious goods • Customers offering fiduciary type services on behalf of other clients. • Nominee arrangements hiding the identity of the UBO • Full discretionary authority provided to an individual who is acting on behalf of another client. • Sudden increase in business activities. • Transactions over EUR100,000	• Investment above Euro 100,000.00	• Non-face-to-face business in non-reputable jurisdictions and high risk countries
Low to Medium	• Reputable jurisdiction (Table 4) • EU member states • Domestic	• Mainstream products/ services • Funds of clients received by bank transfer from Malta, EU or any other reputable jurisdiction	• Investments lower than EUR15K	• Non face-to-face business in reputable jurisdictions
SCDD	• Regulated Entities	• None	• None	• None

Clients falling under this category are extreme and fall beyond the risk appetite of the Company. No business shall be accepted with clients falling under these categories.

ECDD should be undertaken and notified to the MLRO. In case of PEPs, the ECDD procedures in Section 4 need to be followed. In case of high value deposits the Company should obtain evidence of source of funds.

On-going monitoring: The frequency of monitoring clients' transactions would depend upon the category of risk in terms of ML/FT the client falls. It is expected that the following monitoring is undertaken:

Low Risk	**1 year to 3 years**
Medium Risk	**1 year – 18 months**
High Risk	**6 months**

On-going updating of the client profile (re-classification): There might be situations where the client is classified as low in terms of money laundering and financial of terrorism risk but his risk profile changed to high due to his personal circumstances. For example a client becomes a PEP. In such event the name of the client shall be referred to the MLRO and board for reviewing and approval.

4.6. Reliance on Third Parties or other Subject Persons

60. The Company may rely on the CDD carried out by a third party in respect of an applicant for business, but only in circumstances where the third party is subject to the same, or sufficiently similar CDD obligations as the Company. If for any reason it is not possible for the Company to rely on third parties, then the acceptance of the particular client should be discussed with the MLRO and an assessment made by the Company whether it is in a position to fulfil its CDD obligations without reliance being placed on third parties.

61. In the event that the Company relies on a third party for CDD, it is important to remember that the Company shall remain responsible for this CDD. In addition, the Company also remains responsible for the ongoing monitoring obligations on the client.

62. The CDD collected by the third party that is being relied upon by the Company must be immediately available to the Directors, officers and managers of the Company. This information must include:

    a. A record containing the details of the persons on whom reliance is made including the name of the persons, whether legal or natural, identification number or registration number, and the country of residence and address or registered address of such person, together with any other relevant contact detail;
    b. The basis upon which reliance on such persons is made;
    c. A record containing copies of the customer due diligence policies and procedures maintained by the entity on whom reliance is made, together with all the evidence gathered from any sampling carried out in order to ensure that such policies and procedures are carried into effect by the relevant entity or a confirmation to this effect in the letter of comfort/reliance issued by such third party, depending on the profile of the third party on which reliance is being placed;

d. A record containing all the due diligence documentation that has been gathered on the entity being relied upon; and
e. A record containing the details of the business relationship and the transactions undertaken by the clients, including, where necessary, the source of funds.

63. In cases where the Company is relying on a third party, such party has to sign the declaration as found in Appendix 4.

64. The Company can rely on a third party for the purpose of:
- The identification and verification of an applicant for business;
- The identification and verification of a beneficial owner, where applicable; and
- Information on the purpose and intended nature of the business relationship.

65. Notwithstanding, the Company is still responsible for the on-going monitoring measures.

66. Where applicable, the Company shall random check CDD performed by the third party, particularly where there are high risk/enhanced due diligence situations.

67. The Company shall still request the third party on whom reliance is place to:
- Identify of the applicant for business;
- identify of the beneficial owner;
- determine the purpose and nature of the business relationship.

68. In addition, the Company must ensure that the third party is vigilant and has in place effective CDD procedures that are required to evidence the identity of investors/ beneficial owners where relevant.

69. In this regard, a letter of comfort shall be provided by the third party confirming that:
- The third party is licensed/authorised as a relevant financial business or relevant activity. The name of the regulatory body has to be included;
- The third party is subject to anti-money laundering and counter funding of terrorism regulations;
- CDD undertaken on investors is in accordance with AML and funding of terrorism regulations;
- The circumstances when the due diligence needs to be enhanced, such as in case of PEPs;
- No subscription funds are received from a foreign shell bank or from any person or entity named on the lists of known or suspected terrorist, terrorism organisations or other sanctioned persons issued by the United Nations, European Union or US Treasury Department;
- The evidence obtained as part of the CDD is retained for a period of not less than five years from the date on which the client ceases to be a client of the Company;
- The third party shall provide identification and verification data and other relevant documentation on the client to the Company and to any other relevant competent authority immediately upon request.

4.7. Customer Acceptance Policy

70. At the registered office of the Company, the Directors, officers and managers of the Company shall keep and maintain effective customer acceptance policies in respect of every client of the Company, in order to determine and assess whether a client, or its beneficial owner, is a Politically Exposed Person, or is likely to pose a substantial risk of money laundering or terrorist financing.

71. The customer acceptance policy shall include:

i. A description of the type of customer that is likely to pose a higher than average risk, and an assessment of the client in light of these indicators;
ii. The identification of risk indicators such as customer background, country of origin, business activities, products, linked accounts or activities, and public or other high profile positions, as well as an assessment of the client in light of these indicators; and,
iii. An assessment of whether it is appropriate to apply EDD measures, or those measures related to Politically Exposed Persons, to the client.

4.8. General Prohibitions

72. The following relate to prohibitions which have been set in line with the PMLFTR and Company's risk appetite in line with the above:

- No business shall be accepted where the names of the applicant of business is held anonymously or under a fictitious name;

- An applicant for businesses which has been sanctioned by the UN Security Council or the EU shall not be accepted. In this regard, the relative name shall be referred to the MLRO for further action; and

- No relationship shall be established with a shell bank. A shell bank is a financial term that describes a financial institution that does not have a physical presence in any country. In this regard, when establishing a banking relationship with a bank, it is important to ensure that the bank concerned is properly licensed in Malta, EU or in any reputable jurisdiction.

5. Vetting of Employees and Training Requirements

5.1. Due Diligence on Employees

73. Before hiring new employees, the Company is required in terms of the PMLFTR to carry out due diligence on them. In this regard, new employees are required to provide the following, as applicable in line with their role in the Company:

- ID/Passport/Driving Licence for viewing. A copy to be included on HR file;
- Professional references (in case of officers and middle management);
- Qualification (copies of which are to be included on their HR file);
- Recent (not older than 6 months) police conduct certificate; and
- Curriculum Vitae.

5.2. Employee Training

74. All new employees, upon commencement of their work or engagement, shall undertake AML/CFT training program which would normally include an overview of these procedures, thus including the following topics:
- Definition of money laundering and financing of terrorism;
- Overview of the legal framework both international and national;
- Professional obligations under local laws and regulation;
- AML/CFT and CDD procedures; and
- The process for reporting a suspicious transaction.

75. Furthermore a copy of these procedures should also be made available to all new staff for referencing purposes.

76. A refresher course and update to all employees including directors is given at least once a year.

6. Record Keeping and Access to Clients' Files

77. The aforementioned documentation, in relation to CDD, contains sensitive and confidential information. In this regard the access to the files containing such documentation needs to be restricted to the Directors, the Compliance Officer and the person in charge of the client. Disclosure of information (emanating from CDD requirements and/or any confidential correspondence thereto) to third parties is strictly prohibited without the prior written consent from the client, save for the Competent Authorities (FIAU/ MFSA/ Police/ Law Courts).

78. The Company shall keep record of all CDD documentation which has been obtained in line with this Manual and of all the transactions carried at the client during the course of the business relationship. In addition, the following records also need to be held as evidence of compliance with the PMLFTR:
    - internal reports made to the MLRO;
    - reports made by the subject person to the FIAU;
    - a record of the reasons for not forwarding an internal report to the FIAU;
    - a record of AML/CFT training provided, including:
        - the date on which the training was delivered;
        - the nature of the training;
        - the names of employees receiving the training;
        - the results of any assessment undertaken by employees;
        - a copy of any handouts or slides;
    - other important records, including:
        - any reports by the MLRO to senior management made for the purposes of complying with the obligations under the PMLFTR such as recommendations on internal procedures, correspondent banking relationships, PEPs, etc;
        - records of consideration of those reports and of any action taken as a consequence thereof;
        - reports drawn up in relation to an internal audit or assessment dealing with AML/CFT issues.

6.1. Record Keeping Time-frames

79. The following table establishes the period of retention of CDD records in line with the PMLFTR.

Table 7 – Record Keeping

Type of Document	Time frame
CDD Documentation	5 years from when the business relationship is terminated.
Employees' Due diligence documentation	5 years from when the employee resigned or terminated his/her contract of employment
In case of ML/FT STR	5 years from when the suspicious transaction was reported. This period might be extended by the FIAU as required.

Records on transactions in the course of a business relationship or occasional transactions	5 years from when all dealings taking place in the course of the transaction were completed. In the case of an occasional transaction or a series of occasional transactions, the 5 years shall commence from the date on which such occasional transaction or the last of a series of occasional transactions took place.
Records of examinations done relating to large and complex transactions and non-reputable jurisdictions	5 years from when all dealings taking place in the course of the transaction concerned were completed.
Internal reports made to the MLRO and reasons for not reporting same to the FIAU, if any	Indefinitely
Record of AML/ CFT training held	Indefinitely
Other important records including reports made by the MLRO in compliance with the PMLFTR and internal audit reports	Indefinitely

80. Any CDD documentation is to be kept separately from any other documents relating to the client as mentioned above, and in a safe place whereby access is restricted only to the required persons. This is also applicable to electronic documentation, such as scanned documents.

81. The FIAU may request information on clients or STRs filed. Such requests made by the FIAU shall be referred to the MLRO. The FIAU implementing measures stipulate that such information shall be procured within five (5) working days from when the demand is made unless the subject person makes representations justifying why it cannot provide the required documentation within the stipulated time, in which case the FIAU has the discretion to extend the 5 working days as necessary.

7. MLRO and the Reporting of Suspicious Transactions

82. The Board of Directors of the Company shall appoint a money laundering reporting officer (MLRO) to whom information on knowledge or suspicion of money laundering or funding of terrorism shall be reported to and to oversee that the requirements of the PMLFTR and these procedures are being followed. In order to fulfil these duties, the MLRO shall have full access to the clients' files and records.

83. The details of the MLRO or any subsequent changes thereto shall be forwarded to the Director – Financial Intelligence Analysis Unit and the Malta Financial Services Authority for approval as applicable in terms of the PMLFTR.

84. Upon approval of appointment of the MLRO by the MFSA and FIAU, the board of directors shall communicate the name of the MLRO to employees forthwith.

7.1. The Money Laundering Reporting Officer

85. The Board of Directors has appointed Mr Carmine Reho to act as the MLRO of the Company. The contact details of Mr Reho are as follows:

Name	Carmine
Surname	Reho
Designation	MLRO
Address	Skyway, Block C, Office 1, 179, Marina Street, Pieta
Telephone	To be provided
Mobile number	To be provided
Email Address	To be provided

86. The roles and responsibilities of the MLRO are set below:

1. To receive internal reports of suspicious transactions;
2. To evaluate internal reports of suspicious transactions with reference to the available business information;
3. To access available information (both from internal sources, e.g. client files and external sources e.g. web-based information, law enforcement circulars, suspect lists, newspaper reports etc);
4. To make judgments on whether an internal report of a suspicious transaction has merit and should be reported to the FIAU or not as the case may be. In the latter case, the MLRO shall provide a detailed report supporting the rationale why a Suspicious Transaction Reports (STR) has not been filed (see below – Keeping records on STRs);
5. To file STR to the FIAU giving reasons for suspicion;
6. To file internal disclosures that are not reported to FIAU for future analysis, in case a further internal disclosure is made about the same client in the future;
7. To act as the main focal point of contact with law enforcement following disclosure, dealing with both formal and 'informal' requests for additional information;
8. To act autonomously, if necessary, without reference to or influence from management or directors;
9. To maintain a register of internal suspicious transaction reports and STRs (whether reported or not to the FIAU);
10. To keep abreast with money laundering cases and to remain fully up-to-date with anti-money laundering legislation and EU Sanctions issued from time-to-time:
11. The regular generation of management information on internal and external STR reporting trends;
12. Monitoring the internal effectiveness of the anti-money laundering procedures;
13. An awareness of the FATF Non-Cooperative Countries and Territories and other countries that do not have adequate anti-money laundering frameworks in place;
14. An awareness of the content of lists of suspects and sanctions issued by law enforcement agencies (including but not limited to the FIAU) and regulatory bodies (MFSA);

15. Contributing to the maintenance of a continually high level of anti money laundering awareness between training sessions;
16. Maintenance of records on anti-money laundering training;
17. To attend training both locally and abroad (where available) on anti-money laundering and funding of terrorism; and
18. Preparing for and dealing with regulatory visits and inspections.

7.2. Police Investigations and Court Orders

87. Police investigations in connection with a Court case concerning money laundering and funding of terrorism shall be forwarded to the MLRO. The names shall be searched on the Company database and records. In the eventuality that the person being investigated is a client of the Company, relative information pertaining to that client shall be duly forwarded to the Police. The board of directors shall be informed of such events immediately.

7.3. Reporting Suspicious Activity and Transactions

88. In terms of the PMLFTR, the Company is required to file a Suspicious Transaction Report (STR) with the FIAU where it knows, suspects or has reasonable grounds to suspect that a transaction may be related to money laundering or to the funding of terrorism.

89. The submission of an STR should be carried out **within 5 working days from when the suspicion first arose**. As part of the information, persons filing an STR have to provide relevant identification and other documentation in addition to relevant information pertaining to the suspicion.

90. As part of the relevant information, subject person would need to provide information as to why suspicion of money laundering arose. A transaction is seen as suspicious when this is not consistent with that customer's known legitimate business or personal activities or with the normal business for that type of account.

91. Knowledge or suspicions of money laundering or financial of terrorisms raised internally should be forwarded to the MLRO who is responsible for:
    - evaluation of the information provided;
    - giving judgment on whether the information merits to be reported to the FIAU through an STR;
    - acting as the main point of contact with FIAU; and
    - acting autonomously without reference to or influence from management.

92. A subject person who does not satisfy the reporting requirements or fails to submit the required information to the relevant authorities in terms of the PMLFTR shall be liable to an administrative penalty. The FIAU has also the power in terms of the above regulations to impose an administrative penalty on a daily cumulative basis until compliance with the above requirements.

7.4. Procedures for filing a Suspicious Transaction Report

93. The clients' financial behaviour and transactions shall be monitored during the course of their business relationship with the Company. Whilst monitoring activities of the clients, special attention should be paid to large or complex transactions, including unusual patterns of behaviour which do not have apparent or viable lawful purpose and business relationships and transactions with persons, companies and undertakings, including those carrying out relevant financial business or a relevant activity, from a jurisdiction that does not meet the definition of a reputable jurisdiction. An employee, who has identified unexpected changes without reasonable change in profile or a suspicious activity, must inform the MLRO before

the transaction at issue is processed or before further services are performed on the customer's behalf. The following process shall be followed when reporting suspicious activity:

1) The Company's employee concerned shall immediately contact the respective MLRO and file the attached Internal Suspicious Transaction Report enclosed herein as Appendix 5 – Internal Suspicious Transaction Report. Any supporting documentation, as applicable, shall also be attached to the report;

2) The MLRO shall, after evaluating the case in line with the PMLFTR and these procedures, complete and file an online STR from the FIAU website (http://www.fiumalta.org/) if he has knowledge, suspicion or reasonable grounds to suspect the case is related or may be related to money laundering or funding of terrorism activities. In any case such reporting should be done not later than five working days from when the suspicion first arose; and

3) The Company's employee shall refrain from carrying out a transaction that is suspected or known to be related to money laundering or the funding of terrorism until the respective suspicious transaction report has been forwarded to the FIAU. If such situation is not possible or is likely to frustrate efforts of investigating or pursuing the beneficiaries of the suspected money laundering or funding of terrorism operations, the MLRO shall immediately inform the FIAU when such transaction has been effected.

7.5. Confidentiality and Tipping Off

94. All STRs should be reported in a confidential manner and shall not be discussed, mentioned (intentionally and unintentionally) to clients and to colleagues but only to the appointed money laundering reporting officer.

95. One should note that **'tipping off'** is also an offence in terms of the Act. Tipping Off is the act of disclosing information to customers or to third parties that information has been transmitted to authorities or that a money laundering investigation has been carried out on that customer. In doing so, the director or employee of the subject person, would be jeopardizing or likely to jeopardize an investigation or proposed investigation.

96. <u>It is highly recommended that all employees, also through their behavior, should never indicate, suggest or give the impression that a STR has been made or will be made.</u>

7.6. Record Keeping of STRs

97. All internal reports of suspicious transactions received by the MLRO shall be recorded in a logbook by date order. Such reports are to be retained for a period of five years until advised by the authorities that they are no longer needed.

98. Internal suspicious transaction reports which have not been forwarded to FIAU on justifiable reasons shall be also recorded. The MLRO shall also record the reasons for such determinations in writing and, upon inquiry, shall make it available to the FIAU or the supervisory authority acting on behalf of the FIAU in monitoring compliance with the PMLFTR regulations.

7.8. Annual Compliance Report

99. In accordance with the local laws and regulations, the Company is obliged to prepare an annual compliance report as prescribed by the FIAU in order to fulfill

the latter's obligation of monitoring compliance with AML/CFT obligations by subject persons.

100. The annual compliance report requires the completion of general details on the subject persons, as well as other information, as follows:

- information on internal suspicious reports and STRs submitted to the FIAU;
- an overview of the policies and procedures on internal control, risk assessment, risk management and compliance management established by the subject person and their effective implementation;
- an overview of the manner through which the MLRO would have assessed internal compliance, including overall oversight by the internal audit function, where applicable, highlighting any non-compliance findings that may have been identified and corrective measures taken accordingly; and
- information concerning the AML/CFT training attended by the MLRO and any designated employees and AML/CFT training provided to staff members.

101. The Report shall be completed by the MLRO and circulated to the Board of Directors for their approval. Once approved, the Annual Report shall be filed via the FIAU website as detailed above. The Company is required to submit this report to the FIAU by not later than 31st March of every year, covering the previous calendar year.

APPENDICES SECTION

Appendix 1: Definition of Relevant Activity and Relevant Financial Business

'Relevant Activity' means the activity of the following legal or natural persons when acting in the exercise of their professional activities:

(a) Auditors, external accountants and tax advisors, including when acting as provided for in paragraph (c) below;

(b) Real estate agents;

(c) Notaries and other independent legal professionals when they participate, whether by acting on behalf of and for their client in any financial or real estate transaction or by assisting in the planning o execution of transactions for their clients concerning the: -

- Buying and selling of real property or business entities;
- Managing of client money, securities or other assets unless the activity is undertaken under a licence issued under the provisions of the Investment Services Act;
- Opening or management of bank, savings or securities accounts;
- Organisation of contributions necessary for the creation, operation or management of companies;
- Creation, operation or management of trusts, companies; or similar structures or when acting as a trust or company service provider.

(d) Trust and company service providers not already covered under paragraphs (a), (c), (e) and (f);

(e) Nominee companies holding a warrant under the Malta Financial Services Authority Act and acting in relation to dissolved companies registered under the said Act;

(f) Any person providing trustee or any other fiduciary service, whether authorised or otherwise, in terms of the Trusts and Trustees Act;

(g) Casino Licensee;

(h) Other natural or legal persons trading in goods whenever payment is made in cash in an amount equal to fifteen thousand euro (€15,000) or more whether the transaction is carried out in a single operation or in several operations which appear to be linked; and

(i) Any activity which is associated with an activity falling within the paragraphs (a) to (h) above.

'Relevant Financial Business' means:

(a) any business of banking or any business of an electronic money institution carried on by a person or institution who is for the time being authorised or required to be authorised, under the provisions of the Banking Act;

(b) any activity of a financial institution carried on by a person or institution who is for the time being authorised or required to be authorised under the provisions of the Financial Institutions Act;

(c) long term insurance business carried on by a person or institution who is for the time being authorised or required to be authorised under the provisions of the Insurance Business Act or enrolled or required or required to be enrolled under the provisions of the Insurance Intermediaries Act, any business of affiliated insurances carried on by a person in accordance with the Insurance Business (Companies Carrying on Business of affiliated insurance carried on by a cell company and an incorporated cell in accordance with the provisions of the Companies Act (Incorporated Cell Companies Carrying on Business of Insurance) Regulations;

(d) investment services carried on by a person or institution licensed or required to be licensed under the provisions of the Investment Services Act;

(e) administration services to collective investment schemes carried on by a person or institution recognised or required to be recognised under the provisions of the Investment Services Act;

(f) a collective investment scheme marketing its units or shares, licensed or recognised or required to be licensed or recognised, under the provisions of the Investment Services Act;

(g) any activity other than that of a scheme or a retirement fund, carried on in relation to a scheme, by a person or institution registered or required to be registered under the provisions of the Special Funds (Regulation) Act and for the purpose of this paragraph "scheme" and "retirement fund" shall have the same meaning as it assigned to them in the said Act;

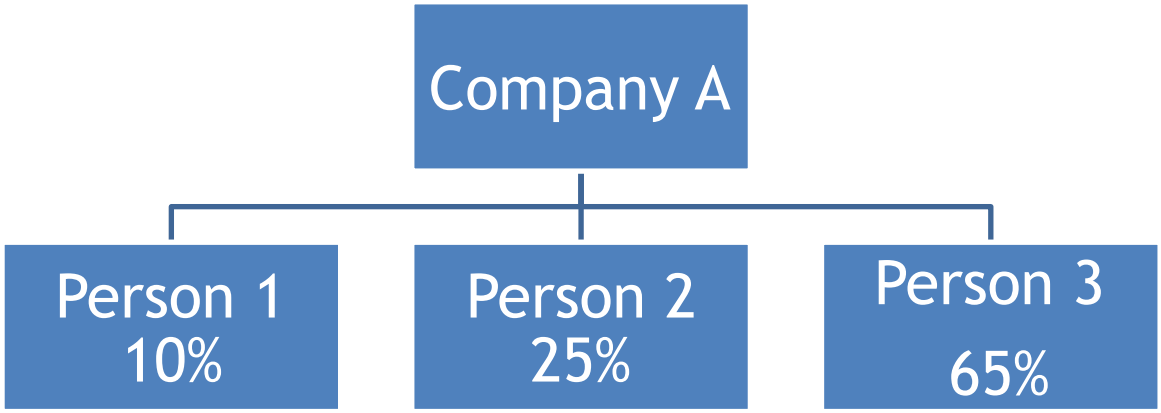
(h) any activity of a regulated market and that of a central securities depository authorised or required to be authorised under the provisions of the Financial Markets Act;

(i) any activity under paragraphs (a) to (h) carried out by branches established in Malta and whose head offices are located inside or outside the Community;

(j) any activity which is associated with a business falling within paragraphs (a) to (i)

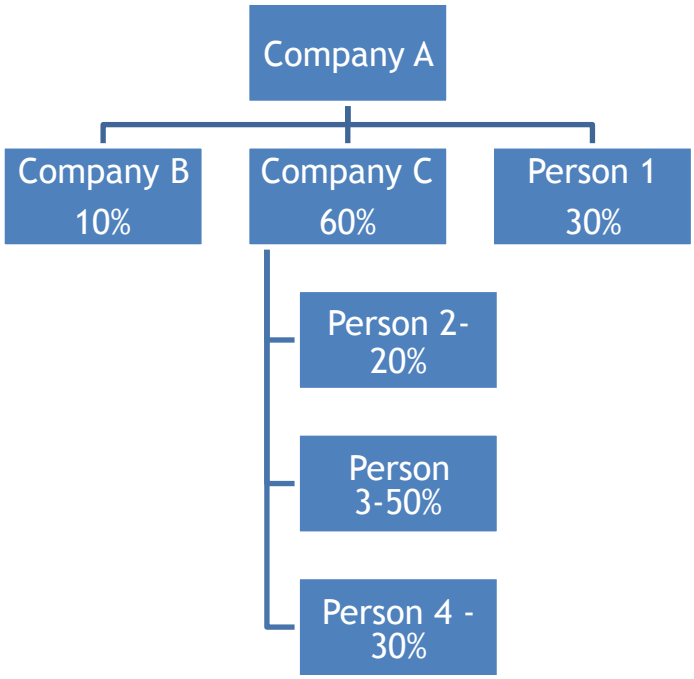
Appendix 2 – Cases of Beneficial Owners including Multi-layered Companies

Case 1



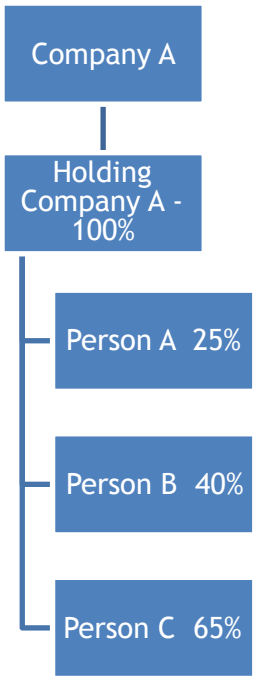
For Case 1 - Person 2 and Person 3 would be subject to CDD

Case 2



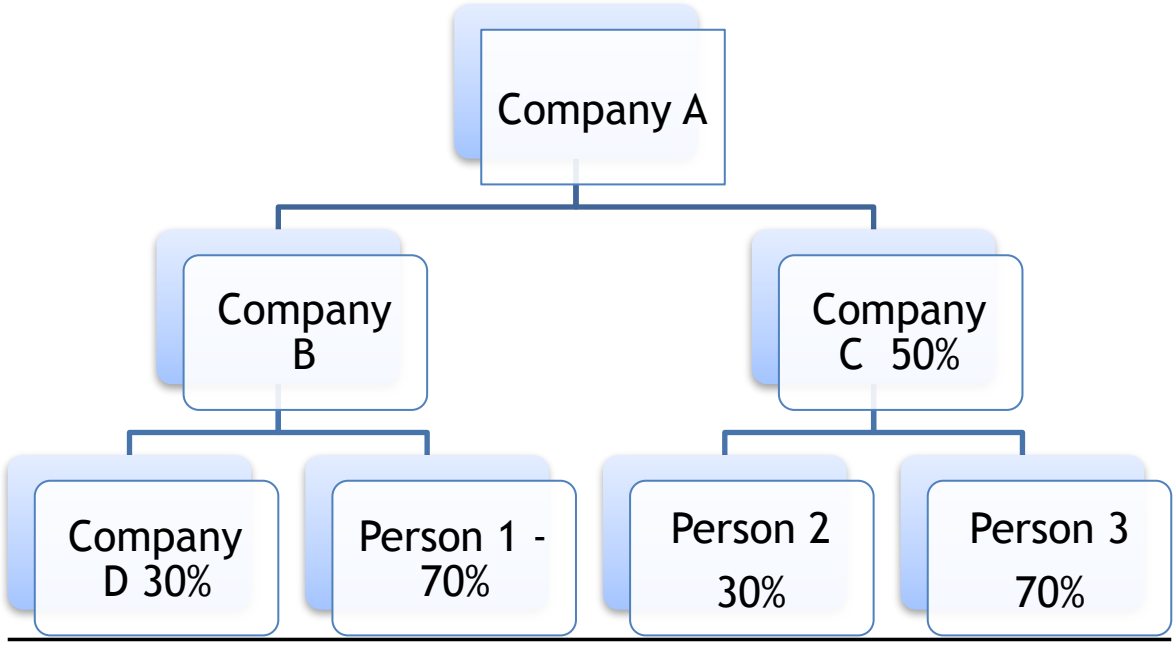
Case 2 – Person 1 and Person 3 qualify. Person 3 ultimately holds 30% in Company A which is above the threshold of 25%

Case 3



In Case 3: Persons A, B, C would qualify as they ultimately hold more that 25% stake

Case 4



In case 4: Persons 1 and Person 3 would qualify. Person 2 ultimately holds 15% stake in Company A.

Appendix 3 - High-Risk and Non-Cooperative Jurisdictions

Non-Cooperative Countries and High Risk Countries **(Source: www.fatf.org)***

Jurisdictions that have strategic AML/CFT deficiencies and to which counter-measures apply
Iran Democratic Peoples's Republic of Korea (DPRK)
Jurisdictions with strategic deficiencies
Bosnia and Herzegovina Ethiopia Iraq Syria Uganda Vanuatu Yemen
Jurisdictions no longer subject to monitoring
Guyana Lao PDR Afghanistan

*** Reference should be made to the latest list published by the FATF available from the following link: (http://www.fatf-gafi.org/topics/high-riskandnon-cooperativejurisdictions/)**

Appendix 4 – Declaration on Third Party Reliance

By signing of this declaration, We (include the name of the relevant financial business or relevant business) _____declare that we have satisfactorily carried out the customer due diligence in line with anti-money laundering and counter funding of terrorism requirements on_____ _____(name of client) residing at _____ _____ _____ and with ID card/Passport number as follows: _____

By means of this declaration, We also confirm and acknowledge that the relative customer due diligence shall be submitted to Abalone Asset Management Ltd immediately but not later than 2 business days from their request.

Name of official at the relevant financial business or relevant activity

Name
Position
Address
Date

Appendix 5 – Internal Suspicious Transaction Report

Name of individual raising the STR	
Designation	
Department	
Client Details	
Name /Company Name	
Address:	
Client number or reference (as applicable)	
Details of the Ultimate Beneficial Owners (name, addresses)	
Names and other relevant details of principals representing the client	
Description of services provided to the client	
Please describe how the suspicious activity, which prompted the report, took place.	

Why is the activity suspicious?	
Which steps have been already undertaken (e.g. own investigations)?	
Name and Signatures of employee raising the report	
Name and signature of the MLRO and date of receipt	
Annex	
i) Documentation relating to the client (and persons representing them) and transaction **ii) Other document proving the ultimate beneficial owner (if existing)**	