IRISH FUNDS INDUSTRY ASSOCIATION

INVESTMENT FUNDS SECTORAL GUIDELINES

Drafted by the Irish Funds Industry Association

- on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing

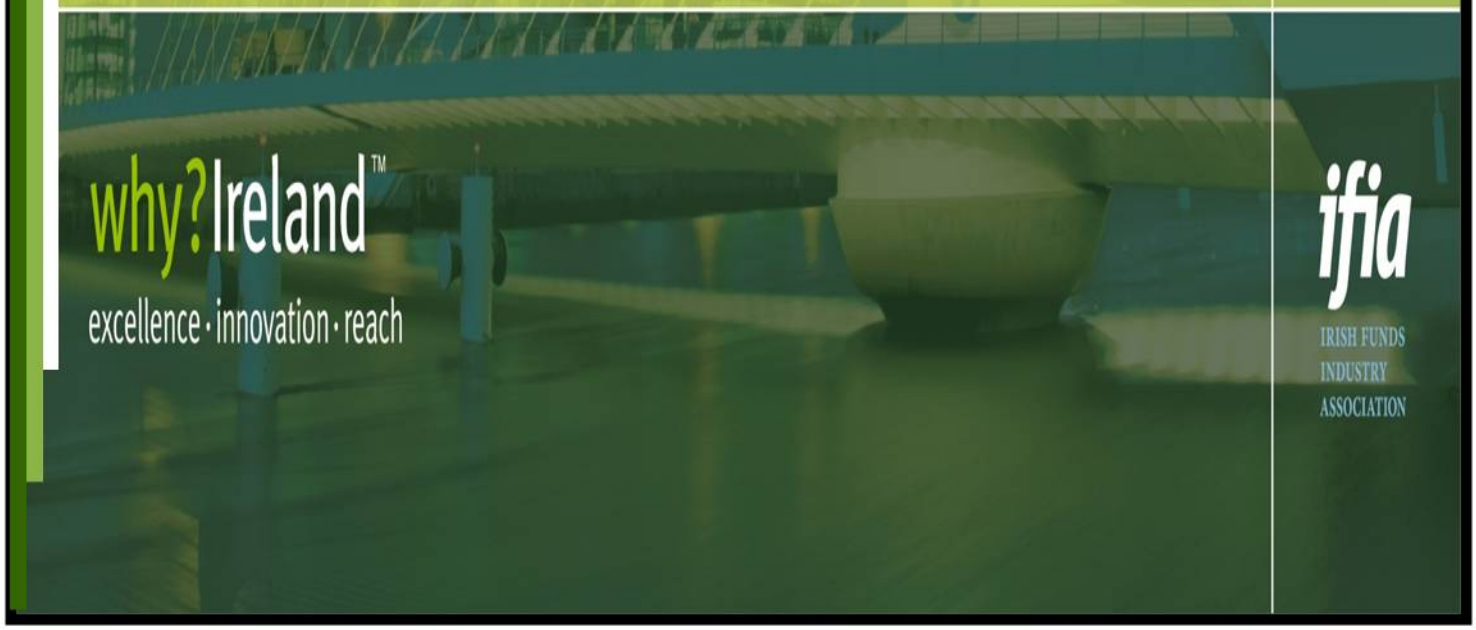


TABLE OF CONTENTS

APPENDICES

1. BACKGROUND

1. These Guidelines should be read in conjunction with the published *Core Guidelines on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing*" ("the Core Guidelines") and reference should be made to the Criminal Justice (Money Laundering and Terrorist Financing) Acts 2010-13 ('The Acts'). These guidelines do not constitute secondary legislation and Designated Persons must always refer directly to the Acts when ascertaining their statutory obligations. These guidelines are subordinate to the Acts and to the Core Guidelines referred to above.

2. The Acts derive from the 3rd EU Money Laundering Directive ('The Directive'), which in turn is based upon the 40 recommendations of the Financial Action Task Force ('FATF') the foremost international body in the fight against money laundering and terrorist financing.

3. A risk based approach is the foundation upon which this Directive is based. By providing for a risk-based approach, the Directive enables Designated Persons (as defined within the Acts) to ensure that measures to mitigate money laundering and terrorist financing are commensurate with the risks identified.

4. As a high level summary, under the Acts, Designated Persons are obliged to:

- **i.** apply Customer Due Diligence (CDD) procedures to identify and verify customers;
- **ii.** identify and, where applicable, verify, the beneficial owners of customers;
- **iii.** monitor the business relationship on an on-going basis and report any suspicions of money laundering and terrorist financing;
- **iv.** apply Enhanced Due Diligence (ECDD) to high-risk investors;
- **v.** determine the source of wealth and of funds for Politically Exposed Persons ("PEPs");
- **vi.** monitor dealings with the customer (to the extent reasonably warranted by risk) by scrutinizing transactions and source of wealth or source of funds for those transactions to determine whether or not the transaction are consistent with the profile of the customer;
- **vii.** promptly report suspicions of money laundering or terrorist financing to the Gardaí and Revenue Commissioners; and
- **viii.** maintain appropriate records, to train staff and to maintain appropriate procedures and controls pertaining to the obligations imposed by the Acts.

Designated Persons are permitted to rely on "relevant" third parties to perform CDD requirements falling under Section 33 ("identification and verification of customers and beneficial owners") and Section 35(1) of the Acts (obtaining information on the purpose and intended nature of a business relationship with a customer prior to the establishment of the relationship).

It should be noted that the Acts do not allow Designated Persons to rely on relevant third parties for aspects of CDD obligations falling outside Section 33 and Section 35(1) of the Acts. In addition, ultimate responsibility for ensuring compliance with the full CDD obligation still resides with the Designated Person that relies on a third party.

The application of the CDD obligations on a risk-based approach provides for better allocation of resources in the fight against money laundering and the financing of terrorism. In line with the concept of a risk based approach, the Acts set out specifically when both enhanced and simplified CDD procedures should be applied to specified investor types.

5. These Guidelines are designed to provide guidance to Designated Persons within the fund industry on a suggested approach to combating money laundering and terrorist financing in light of the Acts.

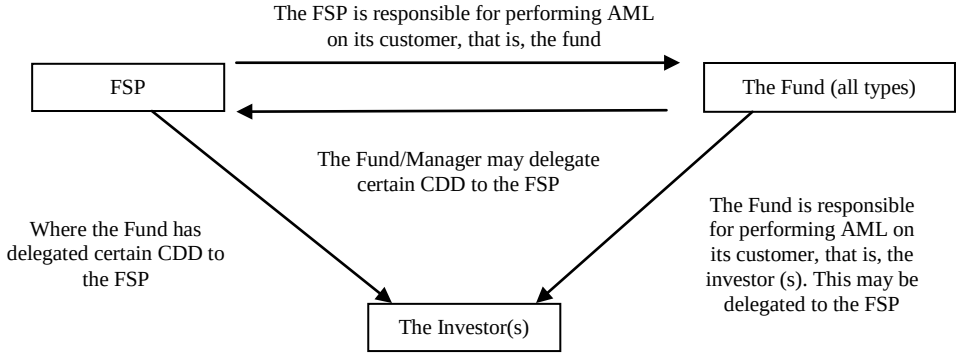
2. RESPONSIBILITIES

6. The adoption and application of appropriate anti-money laundering procedures in relation to investment funds is a process that involves the following:

- **i.** The board of directors and MLRO of the Fund or Management Company (in the case of a unit trust);
- **ii.** The promoter/investment manager (we will refer to both of them as the "Promoter") of the Fund;
- **iii.** The entity responsible for marketing / sale of the Fund; and
- **iv.** The Fund Service Providers (FSP) e.g. Administrator, Trustee/Custodian etc.

Any or all of the above may be a Designated Person as defined in the Acts.

7. The Fund or the Management Company (in the case of a unit trust) is responsible for performing Customer Due Diligence on its customers, the investors. As detailed below, the Fund may delegate certain Customer Due Diligence activities to the FSP. The Fund is the customer of the FSP (see diagram below).



8. The FSP must conduct appropriate due diligence, prior to entering into business with the Fund Promoter. The extent of due diligence will be dependent on whether the Promoter is regulated for AML purposes, if the Promoter is domiciled in the EU or other equivalent jurisdictions etc.

9. Subsequently, an "Agreement" must be entered into with the Fund, the Management Company or the Promoter outlining the respective duties and obligations of the Fund and the FSP. It should be agreed who has contractual responsibility for AML compliance support, verifying the identity of the Fund's investors and other anti-money laundering procedures. These roles should be outlined in an Agreement or SLA.

10. In practice, it is typically the FSP or the Promoter who undertakes Customer Due Diligence of the investors on behalf of the Fund and the FSP is responsible for on-going monitoring.

The Money Laundering Reporting Officer (MLRO)

11. The Core Guidelines elaborate in greater detail on the role and responsibilities of the MLRO. In addition to the FSP MLRO, a Fund MLRO may be appointed. It should be noted that for non-Irish funds there may not be a requirement to appoint an MLRO.

12. A Fund as well as the FSP may have their own respective MLROs. For the avoidance of doubt, the MLRO of the Fund, where appointed, is responsible for suspicious activity reporting and may also be assigned responsibility for reviewing processes, systems, controls, and other matters concerning money laundering and terrorist financing, as they apply to the Fund. On a regular basis, the MLRO of the Fund should provide a report on such aforementioned matters to the Board of the Fund or Management Company.

It is recommended that clearly defined responsibilities are agreed and documented between the FSP MLRO and the Fund MLRO. It is similarly recommended that reporting and notification processes should be agreed between the FSP MLRO and the Fund MLRO including escalation of suspicious transactions (in the absence of tipping off concerns).

It should be noted that the Acts require that *each* Designated Person should report to the Garda Síochána and the Revenue Commissioners their suspicions of money laundering. If an arrangement is proposed where, for example to avoid duplication of reporting, *either* the FSP *or* the Fund reports to Garda Síochána and the Revenue Commissioners, this would need to be preapproved by the Garda Síochána and the Revenue Commissioners. A written record of this arrangement should be maintained by the FSP and/or the Fund.

3. RISK BASED APPROACH TO COUNTER MONEY LAUNDERING

13. The adoption of a Risk Based Approach to counter money laundering and terrorist financing can yield huge benefits for Designated Persons. Applied correctly this approach should allow Designated Persons to be more efficient and effective in their allocation of resources as well as minimizing the burden on investors. Designated Persons should use their judgment, knowledge and expertise in developing an appropriate risk-based approach for their particular business activities (e.g. consideration of the investor type), where allowed by the Acts only.

14. A risk-based approach allows Designated Persons to determine and implement proportionate and appropriate measures and controls to mitigate money-laundering risk. This is more efficient and effective when compared to a 'one-size-fits-all' approach where identical measures and controls are implemented across all investor accounts regardless of their risk profile.

15. A well-designed risk based approach will provide a framework for identifying the degree of potential money laundering (and potential terrorist financing) risks associated with investors and their transactions. It will allow a Designated Person to focus on those investors and transactions that potentially pose the greatest risk of money laundering

16. Outlined below are some considerations which Designated Persons may find useful in developing and implementing a risk based approach to counter money laundering and terrorist financing. The specific details of a Designated Person's risk based process should be determined by its Designated Person's Money Laundering Reporting Officer and Compliance and Business Unit, based on the nature, scale and complexity of its operations.

Customer Due Diligence (CDD)

17. Customer Due Diligence (CDD) shall comprise of the following:

- **i.** Identifying the investor and verifying the investor's identity on the basis of documents, data or information obtained from a reliable and independent source;
- **ii.** Identify any beneficial owner of the investor, and verify the beneficial owner (the extent of verification of any beneficial owner will be determined according to the risk of money laundering or terrorist financing) after applying a risk-based approach. This may include understanding the ownership and control structure of the investor if it is an entity rather than a person;
- **iii.** Prior to the establishment of the business relationship, obtain information on the purpose and intended nature of the business relationship. For the funds industry the provision of an application form indicates the investors' intention, that is, an investment into the relevant fund.
- **iv.** Conducting on-going monitoring of the business relationship including to the extent warranted by the risk, scrutiny of transactions scrutinising the source of wealth or of funds for those transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the institution's or person's knowledge of the customer, the business and risk profile.

18. CDD measures shall be applied in the following cases (please refer to Section 33 of the Acts for full details on these cases):

i. prior to establishing a business relationship with the investor; or

ii. during the establishment of a business relationship with the investor if the Designated Person has reasonable grounds to believe that:

- **a.** Verifying the identity of the investor prior to the establishment of the relationship would interrupt the normal conduct of business; and
- **b.** There is no real risk of money laundering or terrorist financing occurring provided that the verification is completed as soon as practicable after the initial contact

It should be noted that no investor payments, including but not limited to redemptions or distributions, should be made until the appropriate due diligence is completed.

iii. when carrying out occasional transactions, whether the transaction is carried out in a single operation or in several operations which appear to be linked;

iv. when there is a suspicion of money laundering or terrorist financing, regardless of any derogation, exemption or threshold;

v. when there are doubts about the veracity or adequacy of previously obtained investor identification data.

4. KEY COMPONENTS OF A RISK BASED APPROACH

19. In the Investment Funds sector, the most common and applicable risk criteria for a Designated Person or Intermediary for measuring money laundering risk are Country Risk and Customer Risk. In each case, these primary risk criteria may be modified by further additional risk variables as outlined further below.

GEOGRAPHIC RISK ASSESSMENT

20. Notwithstanding that a jurisdiction may be included on a list of equivalent jurisdictions issued by the Minister for Justice the following additional geographic risk assessment factors would also be relevant for investors investing directly from such jurisdictions. This is not exhaustive and Designated Persons may wish to consider other factors.

- **i.** FATF Membership.
- **ii.** Gulf Co-operation membership.
- **iii.** whether jurisdiction is noted in EU, UN or OFAC sanctions lists.
- **iv.** whether jurisdiction is known as a drug producing country.
- **v.** whether the jurisdiction is noted by the OECD as a tax haven and whether it is has implemented or committed to the "internationally agreed tax standard".
- **vi.** perceived level of (endemic) corruption etc [the Corruption Perceptions Index produced by Transparency International (http://www.transparency.org) may be a useful resource].
- **vii.** political stability.
- **viii.** evidence of relevant (public) criticism of a jurisdiction, including FATF (and other) advisory notices.
- **ix.** independent and public assessment of the jurisdiction's overall AML/CTF regime

Customer Risk

21. Customer risk varies according to customer type.

As an example, the following customer types are usually considered to be lower risk:

- **i.** regulated credit and financial institutions;
- **ii.** pension schemes;
- **iii.** companies listed on a regulated market.

22. The following customer types are usually considered to be higher risk:

- **i.** unregulated non-profit organisations;
- **ii.** trusts with complex structures in high risk jurisdictions;
- **iii.** unlisted companies.
- **iv.** 'gatekeeper' accounts operated by accountants, lawyers etc. operating for customers where the identity of the investor is not disclosed;

23. In addition, Designated Persons should consider the factors below when determining customer risk:

- **i.** Politically Exposed Persons ("PEPs");

ii. the known business of the investor;

iii. entities with no physical place of business ('shell entities');

iv. investors with P.O. Box rather than full addresses.Where postal boxes are supplied instead of full addresses, the Designated Person should consider whether this is standard practice for the investor's country of residence or whether the practice is suspicious.

v. whether the customer or those persons who may exercise control over the customer's investments (e.g. the customer's directors, beneficial owners, authorised signatories) are Politically Exposed Persons.

Refer to the matrix in Appendix 1, which gives guidance on the documentation which may be obtained, based on the risk categorization of the investor.

Additional Risk Variables

24. A Designated Person's risk based approach methodology may also take into account additional risk variables, specific to a particular investor or transaction. These variables may increase or decrease the perceived risk posed by a particular investor or transaction. It should be noted that some of these variables may only become apparent during the course of the business relationship, others may be apparent prior to the commencement of the business relationship. These risk variables include:

i. the level of investment by the particular investor or size and frequency of transactions undertaken (e.g. unusually high levels of investments and transactions compared to what might reasonably be expected of investors with a similar profile).

ii. the closeness of the investor relationship. Long standing relationships involving frequent investor contact throughout the relationship may present less risk from a money laundering perspective.

iii. whether the investor has been introduced by a Third Party-see Section 7 'Reliance on Third Parties to undertake Due Diligence'.

iv. the use of intermediate corporate vehicles or other structures that have no apparent commercial or other rationale or that unnecessarily increase the complexity or otherwise result in a lack of transparency. The use of such vehicles or structures, without an acceptable explanation, increases the risk.

v. the level of regulation or other oversight or governance regime to which an investor is subject in its home jurisdiction.

vi. the Designated Person's familiarity with a jurisdiction, including knowledge of local laws, regulations and rules, as well as the structure and extent of regulatory oversight, as the result of the financial institution's own operations within the jurisdiction.

Note: The weight given to these primary risk criteria and the additional risk variables in assessing the overall risk of potential money laundering by a specific investor is discretionary. Application of the above referenced risk criteria and risk variables is intended to provide a strategy for managing potential money laundering risks primarily aimed at high risk investors.

Product Risk

25. A risk-based approach may include determining the potential risks presented by products and services offered. For example, a close-ended fund, by its nature, may be a less attractive vehicle for laundering money than an open-ended fund. Investment in such funds may pose a lower money laundering risk.

26. Each Designated Person should document the rationale behind its individual risk based approach to money laundering and in line with good practice periodically (no less frequently than annually) review its risk assessment approach.

What level of Customer Due Diligence should be applied?

27. The Acts closely define the circumstances in which Simplified Customer Due Diligence can apply and in which Enhanced Customer Due Diligence must apply. It is suggested that for the range of customers which fall within the Standard Customer Due Diligence bracket that the Designated Person may determine whether they are lower or higher risk after having assessed the Country Risk, Customer Risk and other risk variables.

Simplified Customer Due Diligence (SCDD)

Section IV (G & H) of the Core Guidelines gives further information on SCDD.

Standard Customer Due Diligence

28. The Designated Person may apply standard due diligence in situations where based on their risk assessment the investor does not fall into either the simplified or enhanced categories as outlined in the Acts. The level of Standard Customer Due Diligence applied will vary based on a risk assessment of investors within this category i.e. lower or higher risk. Appendix 1 of these Sectoral Guidelines provides general guidance on the documentation, which a Designated Person may request, when applying a range of standard Customer Due Diligence to prove identity of an investor, using a risk based approach.

Non Face to Face-Individuals

29. It is unusual for Designated Persons to have face-to-face contact with fund investors. S33 (4) of the Acts details one or more additional measures which must be carried out where a customer who is an individual does not present to the Designated Person for face to face verification of the customer's identity. While there is some discretion as to which of s.33(4)'s list of possible additional measures will be applied ("one or more") at least one additional measure is required.

Enhanced Customer Due Diligence (ECDD)

30. Section IV (I) of the Core Guidelines gives further information on ECDD.

5. APPLICATION OF A RISK BASED APPROACH TO VERIFICATION AND ONGOING MONITORING

Existing investors

31. Under Section 33(1) (d) of the Acts, Designated Persons are obliged to conduct CDD for existing customers under Section 33(2) and, where applicable, Section 33(4) of the Acts, where Designated Persons have reasonable grounds to doubt the veracity or adequacy of documents or information previously obtained either under the Acts or under the Criminal Justice Act 1994 or administrative arrangements operated by the Designated Person prior to the Criminal Justice Act 1994.

Obtaining new investor information for existing investors

32. A Designated Person should be aware of certain trigger events, which may require application of additional CDD measures in relation to existing investors pursuant to section 33(1) of the Acts. Such trigger events should be determined by a Designated Person in line with its existing risk control measures. Examples of trigger events are outlined below:

i. Information is received by the Designated Person that warrants a review of the investor account and potentially the investor falling into a higher than standard risk category e.g. the investor status changes to a PEP as a result of screening or information sourced by the Designated Person.

ii. Information is received by the Designated Person regarding changes to the investors' details, which may warrant a review of the investor account e.g. change of address for an individual, change of name for a corporate entity, notice that the investor is deceased etc.

Need for on-going monitoring

33. Section 35(3) of the Acts details the requirements for ongoing monitoring of the business relationship between the Designated Person and all investors (including where the Designated Person has relied on a relevant third party to meet its other CDD obligations). Ongoing monitoring of investor accounts and reporting of any suspicions of money laundering or terrorist financing are key components of a risk-based approach to combating money laundering and terrorist financing. A Designated Person should be aware that money laundering and counter terrorist financing risks for investors may only become evident once the investor has begun transacting through the investor account.

34. The levels of monitoring required will vary depending on the type of fund the investor has invested in and the risk profile of the investor. Depending upon the level of investor transaction activity and the deemed risk of potential money laundering or terrorist financing, following risk based assessment, monitoring of investor accounts by a Designated Person may involve some form of process whereby all or a sample of transactions are monitored against pre-determined risk parameters.

35. The Designated Person's monitoring of investor accounts, including transactions processed and where appropriate enquiry into the source of wealth or of funds for transactions (to the extent warranted by the risk), seeks to ensure consistency with the Designated Person's knowledge of the investor account and its risk profile of each investor account.

6. GENERAL APPROACH TO IDENTIFICATION AND VERIFICATION OF IDENTITY

Identification

36. Appendix 1 and Appendix 2 of the Core Guidelines deal in detail with identification and verification procedures and this section should be read in conjunction with the core Guidelines Appendices, as well as with the Acts. Section 33(1) indicates that identification by a Designated Person of the customer and all beneficial owners (except where SCDD is applicable), must occur:

i. prior to the establishment of a business relationship with the customer

ii. prior to carrying out or assisting to carry out a single transaction, or a series of transactions that are or appear to be linked to each other, on behalf of a customer

iii. prior to carrying out any service for the customer, if the Designated Person has reasonable grounds to believe that there is a real risk that the customer is involved in, or the service sought by the customer is for the purpose of, money laundering or terrorist financing, based on circumstances outlined in Section 33(1)(C) of the Acts.

iv. prior to carrying out a service for an existing customer, where there are doubts about the adequacy or veracity of documentation or information previously obtained (see Sections 51-55 above).

Identification of the customer

37. The customer is the person/entity named on the Fund share register (refer to point 7).

Identification of the beneficial owner

38. The identity of the beneficial owner may be obtained from the following (the below is not an exhaustive list. It is for each Designated Person to decide how they identify any beneficial owners):

i. As per the application or subscription form – either as the name on the share register or within the detail of the application form;

ii. On the basis of documentation received;

iii. On the basis of correspondence received from the investor.

Verification

39. Section 33(1) of the Acts indicates that verification by a Designated Person of the customer and (where applicable) the beneficial owner should occur as noted in paragraph 56 above, however under Section 33(5) of the Acts it states, *notwithstanding s33(1)(a)* that a Designated Person may verify the identity of a customer or beneficial owner during the establishment of a business relationship if the Designated Person has reasonable grounds to believe that:

i. verifying the identity of the customer or beneficial owner prior to the establishment of the relationship would interrupt the normal conduct of business, and

ii. there is no real risk that the customer is involved in, or the service sought by the customer

is for the purpose of, money laundering or terrorist financing

but the Designated Person shall take reasonable steps to verify the identity of the customer or beneficial owner "as soon as practicable".

40. Section 33(5) of the Acts is of particular relevance to the funds industry as it is common practice in the funds industry to open investor accounts and accept subscriptions upon receipt of a valid application form and, as a safeguard against money laundering and terrorist financing to withhold payment of redemptions and dividends until full anti-money laundering documentation and information is received. When determining its AML/CTF policy for opening investor accounts and accepting subscriptions in cases where full AML/CTF documentation or information may not have been received, the Fund (or the FSP as appropriate) needs to ensure that its policy is consistent with Section 33(1) and Section 33(5) of the Acts.

41. In particular, the Fund or FSP should specify in its AML/CTF policy how the following controls are applied to new account openings to assess whether or not the new account/investor presents a risk of money laundering or terrorist financing:

a. <u>Prior to account opening</u>

- **i.** risk assessment of new investors e.g. by considering customer risk and country risk.
- **ii.** assessment of information and documentation provided by investors to ensure that it meets minimum requirements e.g. fully completed application form, authorised signatory list, etc.
- **iii.** the Fund (or FSP's) policy should specify circumstances in which additional AML/CTF documentation or information may be identified and/or required prior to account opening and acceptance of subscriptions.
- **iv.** all new investors will be screened against applicable sanction lists and PEP lists. The policy should also specify the action to be taken in the event of valid hit.

On the basis of:

- **i.** identification of the customer and where SCDD is not applicable all beneficial owners and/or
- **ii.** initial documentation received and/or
- **iii.** various screening mentioned above

the Fund or FSP will determine:

- **i.** whether there is any real risk of money laundering or terrorist financing
- **ii.** whether the customer and all beneficial owners where SCDD is not applicable have been sufficiently identified to allow the account to be opened and initial investment to be placed.

b. <u>After account opening</u>

The Fund or FSP will proactively:

- **i.** request any outstanding information and documentation required from the new investor as indicated in the Fund or FSP's policy.
- **ii.** assess any additional information and documentation received from the investor and provide feedback as soon as appropriate.

iii. process transactions according to its policy for investors with incomplete information and documentation on file. In all cases, payment of redemptions and dividends will not take place until full AML/CTF information has been received.

iv. on-going monitoring of the new investors' transactions will be performed. This may include on-going screening checks, source of funds and source of wealth checking, if deemed appropriate by the Fund or FSP on a risk assessment basis in relation to standard customers, or as a strict obligation pursuant to amended s.37(4) of the Acts in relation to customers who have become PEPs.

c. Outstanding Customer Documentation

a. On a regular basis the FSP and Fund (it is up to each FSP and Fund to determine the timing of this) will review the AML report/data in order to assess the following for those customers who have not provided all required AML documentation;

i. the type of customer;

ii. the jurisdiction of the customer;

iii. the nature and quantity of outstanding documentation;

iv. the level of interaction with the investor and how long has the documentation been outstanding.

Based on the above the Fund or FSP will determine on the basis of the delay what additional action is appropriate. This additional action could include, but is not limited to, any of the following on an individual basis or collectively:

i. internal escalation within the Fund or FSP and agreement of an appropriate course of action.

ii. escalation to the MLRO of the Fund or Board of Directors of the Fund and agreement of an appropriate course of action.

In line with S33(8) of the Act failure on the part of the investor to provide the necessary customer due diligence documentation or information will require the Fund to take the following action;

i. Cessation of all services including the acceptance of additional subscriptions and the issuance of dividends;

ii. Discontinuance of the business relationship with the customer.

The FSP may also consider submitting a suspicious transaction report to the Garda Siochana and Revenue Commissioners under section 42(4).

When determining at what point in the CDD process to consider additional actions as outlined above, the Fund or FSP should consider the real risk of money laundering or terrorist financing. As risks may vary considerably according to the nature of the fund, the extent of missing documentation, the investor type, the history of correspondence with the investor and the investor's countries of registration, it may be appropriate to specify different "defined time-frames" and actions according to different risk categories. The escalation procedure and agreed actions need to be clearly documented.

The above assessment will be specified in more detail in the Designated Persons AML/CTF policy.

7. RELIANCE ON THIRD PARTIES TO UNDERTAKE DUE DILIGENCE

Introduction

42. Section V of the Core Guidelines gives detailed guidance on Reliance on relevant third parties and should be reviewed in its entirety.

43. The Acts permit a Designated Person to rely on certain designated third parties to complete CDD. However, the Designated Person must be cautious when relying on third parties as the Designated Person remains liable under Sections 33 and 35(1) for any failure by the third party to apply these measures**.** In addition, a Designated Person must undertake on-going monitoring of all investors including where it has relied upon a third party to meet its CDD obligations.

44. In summary, providing that certain criteria are met a Designated Person (e.g. the Fund, fund promoter or FSP) can rely upon third parties to carry out their CDD obligations falling under Section 33 ("identification and verification of customers and beneficial owners") and Section 35(1) of the Acts (obtaining information on the purpose and intended nature of a business relationship with a customer prior to the establishment of the relationship).

The Designated Person might consider the following prior to placing reliance on a 'relevant third party':

a. the Designated Person has confirmed that the third party is a "relevant third party" as defined by the Section 40 of the Acts by verifying the third party's regulatory status and reviewing any publicly available information or negative news regarding its compliance standards.

b. the results of the Designated Person's risk assessment of the designated jurisdiction (not withstanding that the country may be a designated jurisdiction, further review may be performed) where the third party is carrying on business.

c. any prior experience the Designated Person has had in relying upon the third party, including the promptness and adequacy of documents delivered by the third party on request.

d. the ongoing results of any additional due diligence carried out by the Designated Person upon the third party.

i. there is a written arrangement in place between the Designated Person and the relevant third party dealing with the following:

- the Designated Person may rely on the relevant third party to apply the measures detailed in section 33 or 35(1).
- the relevant third party will forward to it, as soon as practicable after a request from the Designated Person, any documents or information obtained by the relevant third party in applying the measures. Some 'Section 31' countries are known to have 'banking secrecy' legislation which may inhibit or preclude the transfer of documentation or information to third parties without the express consent of the underlying customer. Consequently, before choosing to rely on relevant third parties in such jurisdictions, the Designated Person must satisfy itself that the relevant third party will provide all documentation and information directly to it, as soon as practicable following a direct request from the Designated Person. If the arrangement contains any reference to the disclosure of documentation and information being subject to local law restrictions, court orders, etc., or if the Designated Person has reasonable cause to believe the arrangement would be subject to such terms, even if not documented in the arrangement, such arrangements would be invalid for the purposes of Section 40 of the CJA.
- that the third party will retain the records for a period of at least five years

after the business relationship has ended.

- the AML/CTF regulations to which the third party adheres.
- the group of customers for whom the confirmation is being given (e.g. all investors in a fund, named investors, etc).
- that the third party has verified the identities of the customer and identified the beneficial owner(s) of the customer (extent of verification of the beneficial owner will be dependent upon the assessment of risk).
- the purpose and intended nature of the business relationship between the Designated Person and the customer. In the context of the funds industry the funds customer will have completed an application form, thus the purpose and intended nature of the business relationship is clear.

In addition to the above, the Designated Person may wish to request further confirmations from the third party.

The Core Guidelines also mention that the Designated Person may undertake a review of the third party's AML/CTF policies and procedures and level of compliance with the Acts. Where judged appropriate, such a review may form part of additional due diligence carried out by the Designated Person.

It should be noted that the Designated Person retains responsibility for ensuring that its CDD obligations have been met. Section 40(5) of the Acts notes that "A Designated Person who relies on a relevant third party to apply a measure under section 33 or 35(1) remains liable, under section 33 or 35(1), for any failure to apply the measure".

Circumstances in which due diligence is often performed by a third party

45. Reliance on relevant third parties occurs when an entity, other than the Designated Person, performs certain CDD controls on a customer and the Designated Person chooses to rely upon those controls. Unlike section 8 below 'Nominee and Intermediary Investors', an arrangement as detailed above must be in place before the Designated Person can rely on the relevant third party.

46. Detailed below, are some common circumstances where, for the funds industry, due diligence may be performed by a relevant third party. This should not be considered to be an exhaustive list.

i. a Distributor or intermediary is appointed by the fund to carry out CDD.

ii. a relevant third party is appointed as an Advisor by the investor, e.g. as a broker or independent financial advisor, and undertakes AML/CTF controls upon the investor as part of the third party's normal business requirements.

Group Introductions

47. Section V of the Core Guidelines gives general information regarding group introductions. Where a customer is introduced to a Designated Person by a relevant third party within the same group of companies as the Designated Person, it is not necessary for the customer's identity to be re-verified by the Designated Person, provided that:

i. there is a written arrangement between the introducing group company and the Designated Person. It is recommended that this arrangement contains similar

confirmations to those recommended in para 69 above;

ii. the introducing group company, which carried out the CDD measures upon the customer, meets the definition of a relevant third party.

iii. the CDD measures required to be carried out by the introducing group company are consistent with the AML / CTF legislation within the relevant group company's jurisdiction and the legislation / regulation applied by the introducing group company is named in the arrangement.

iv. the relevant documents and information collected by the group company in relation to the customer are capable of being reproduced in written form in the State. [See Section 11 of these Guidelines for details on Record Keeping.]

Business Acquisitions

48. Section V of the Core Guidelines discusses situations where a Designated Person acquires the business and customers of another Designated Person/administrator. In the funds industry, this happens most often when a fund is converted from one Administrator to another.

49. In business acquisitions, the acquiring Designated Person should:

i. obtain originals or copies of any documents or information used by the outgoing Designated Person/administrator to perform CDD upon the customers.

ii. seek a confirmation from the fund promoter or outgoing Designated Person/administrator that appropriate CDD controls have been carried out upon the customers. This confirmation may incorporate some of the statements contained in the third party written arrangement detailed in para 69.

iii. risk assess the fund promoter or outgoing Designated Person/administrator using the criteria discussed in para 64 when determining how much reliance it is reasonable to place upon the confirmations provided by the fund promoter or third party

iv. perform some sample testing of the documents and information provided by the outgoing Designated Person/administrator to verify whether the CDD upon the customers has been performed to an acceptable standard.

50. As risk assessment and CDD policies may differ between different Designated Persons, it may be helpful for the acquiring Designated Person to obtain an understanding of the outgoing Designated Person/administrator's CDD policies. The Designated Person should then consider the materiality of any differences identified and whether there is a requirement for additional CDD measures to be carried out upon the customers.

51. In the event that:

i. sample testing of the CDD of existing investors indicates that AML/CTF procedures may not have been carried out to an appropriate standard; or

ii. the investor records are not accessible; or

iii. the acquiring Designated Person suspects that the customers are engaged in money laundering or terrorist financing please refer to section 10 below in terms of what those obligations are.

Where the outgoing FSP has relied on third party arrangements, the incoming FSP must ensure that the third party will provide the AML/CTF documentation and information it has collected for the customers as soon as practicable upon a request from the incoming FSP (or the Fund).

The acquiring Designated Person should perform its own CDD of customers as appropriate, to address the perceived issues as soon as practicable.

8. NOMINEE AND INTERMEDIARY INVESTORS

52. An investor would be considered to be investing as a nominee or intermediary where there is an indication or assumption that the investor is transacting on behalf of its underlying clients rather than transacting on its own behalf.

53. As detailed in the Core Guidelines, in conducting a risk based assessment of such investors, a Designated Person must take into account whether there is a legitimate business reason for the use of the account and whether the account is owned or controlled by a regulated financial entity that is a 'Specified Customer'. Such analysis is a prerequisite to determining the appropriate level of customer due diligence to be applied. In determining the level of CDD to apply the Designated Person should consider the following (this list is not exhaustive):

- **i.** whether the nominee or intermediary is a regulated financial institution;
- **ii.** whether the nominee or intermediary is wholly owned by a parent company which is a regulated financial institution;
- **iii.** Whether the nominee or intermediary or its parent company is located in a designated country.

54. Please refer to Appendix 3 for details on some sample nominee or intermediary scenarios that may occur in the Fund industry; suggested CDD approaches that a Designated Person may wish to apply are given. This is not an exhaustive list and FSPs would be expected to document and justify approaches adopted.

9. POLITICALLY EXPOSED PERSONS (PEPS)

See Section IV of the Core Guidelines for further details on PEPs, e.g. definition of a PEP, etc.

55. Designated Persons are required, on a risk-sensitive basis, to:

- **i.** have appropriate risk-based procedures to determine whether a customer or a beneficial owner is a PEP.
- **ii.** obtain appropriate senior management approval for establishing a business relationship with such a customer, before the relationship is established;
- **iii.** take adequate measures to establish the source of wealth and source of funds which are involved in the business relationship or occasional transaction; and
- **iv.** conduct enhanced on-going monitoring of the business relationship.

These measures will also apply where the Designated Person relies on a Relevant Third Party to perform Customer Due Diligence.

56. Establishing whether individuals or legal entities qualify as PEPs is not always straightforward and can present difficulties. The Fund Designated Person would typically consider inserting relevant language into the Fund Subscription Documents for the customer to disclose if they are a PEP. Where the customer is a PEP, or has become a PEP, the customer's source of wealth and funds should be determined in accordance with S37 of the Acts

57. In the situation where the Designated Person considers that there is an increased risk that it may have investors who are PEPs, electronic tools are available, via third-party vendors, which can be employed to compare the names of investors within record keeping systems against the vendor's databases of known PEPs. It may also be advisable to consult relevant reports and databases on corruption risk published by specialised national, international, non-governmental and commercial organisations.

58. Investors may not initially meet the definition of a PEP. The Designated Person should be alert to public information relating to possible changes in the status of its investors with regard to political exposure, and, where new information arises, should determine an appropriate course of action.

10. SUSPICIOUS TRANSACTIONS

59. See Section VII of the Core Guidelines for more detail on when and how reports of suspicious transactions must be made and the necessary internal procedures to support the reporting process.

60. There is a statutory obligation on all persons acting on behalf of a Designated Person, including a FSP, to report, to An Garda Síochána and the Revenue Commissioners, knowledge, suspicions or reasonable grounds for suspicion, that another person has been or is engaged in an offence of money laundering or terrorist financing.

61. FSPs, and other Designated Persons, may choose to adopt internal procedures under which persons involved in the conduct of the Designated Person's business are required instead to report their suspicions internally to, for example, a MLRO, and that the obligation then falls on the MLRO to report to An Garda Síochána and The Revenue Commissioners.

62. The following are some examples of situations that may warrant further investigation. These are only indicative in nature and should not be considered to be an exhaustive list of suspicious transactions (please refer to Section 42(4) of the Acts). Further, the fact that certain transactions display any of the following characteristics, may not always imply that actual money laundering activities are being conducted:

Sales and Dealing Staff

63. Investors in a Fund (individuals, corporations, trusts…) for whom verification of identity proves unusually difficult; who are reluctant to provide the requested information to verify their identity; attempt to reduce the level of information provided to the minimum or provide information that is misleading or difficult to verify.

64. Communication difficulties could be a possible indicator of suspicion, Investor / Intermediary cannot be contacted at the contact details provided (e.g. business address, contact numbers on headed paper, etc). Returned mail and Hold Mail requests could be considered suspicious, as could an on-going preference shown by the Investor / Intermediary to communicate only by mobile phone or via the use of unrelated internet search engine mailboxes (i.e. to an address that cannot be easily identified as being that of the investor).

65. Unexplained inconsistencies arising from the process of identifying or verifying the investor (for example, regarding previous or current country of residence, country of issue of the passport, countries visited according to the passport and documents furnished to confirm name, address and date of birth).

66. An account for which several people have signing authority, yet these people appear to have no relationship with each other (either family ties or business relationship).

67. Investors introduced by an overseas bank, affiliate or other investor where both the investor and introducer are based in jurisdictions where production of drugs or drugs trafficking may be prevalent. Also investors based in Non-cooperative jurisdictions as per the FATF report.

68. An account opened by a legal entity or an organization that has the same address as other legal entities or organizations and for which the same person or persons have signing authority, where there is no apparent economic or legal reason for such an arrangement (for example, individuals serving as company directors for multiple companies headquartered at the same location, etc.).

69. Any transaction in which the counterparty to the transaction is unknown and cannot be identified

using reasonable means.

Intermediaries

70. Any apparent unnecessary use of an intermediary in the transaction.

Dealing patterns

71. A large number of security or fund transactions across a number of jurisdictions.

72. Buying and selling of a security or fund with no discernible purpose or in circumstances which appear unusual, e.g. churning at the investor's request. The exception being in a money market fund where this practice is not unusual or suspicious.

73. The subscription, redemption, exchange or transfer of amounts that fall consistently just below threshold and reporting levels.

74. Regarding non-profit or charitable organisations, financial transactions for which there appears to be no logical economic purpose or in which there appears to be no link between the stated activity of the organisation and the other parties in the transaction.

75. Accounts that receive relevant periodical subscriptions and are dormant for other periods. These accounts are then used in creating a legitimate appearing financial background through which additional fraudulent activities may be carried out.

76. A dormant account containing a minimal sum suddenly receives a subscription or series of subscriptions followed by daily cash withdrawals that continue until the total subscribed amount has been removed.

Abnormal transactions

77. A number of small transactions held by the same counterparty in small amounts of the same security, when the proceeds are being credited to an account different from the original account.

78. The size of the investment does not tie with the occupation (if stated) of the investor.

79. With the exception of Money Market Funds, early redemptions from a Fund could be deemed suspicious, especially if the investor seems willing to accept a short-term loss and is willing to incur large redemption penalties (in comparison to any gains that may have been made).

80. Any transaction in which the nature, size or frequency appears unusual, e.g. early termination of packaged products at a loss due to front end loading; early cancellation, especially where cash had been tendered and/or the refund cheque is to a third party.

81. Transfer of investments to apparently unrelated third parties, (with the exception of Funds on which a secondary market is known to operate. Such transfers can be quite common and permissible provided the Transfer Agent has ensured the appropriate investor identification checks have been completed on both parties to the transfer, before the transfer has been completed on the Transfer Agent's system).

82. Transactions not in keeping with normal practice in the market to which they relate, e.g. with reference to market size and frequency, or at off-market prices.

83. Other transactions linked to the transaction in question which could be designed to disguise money and divert it into other forms or to other destinations and/or beneficiaries.

Payments

84. A number of transactions by the same counterparty in small amounts of the same security, each purchased for cash and then sold in one transaction.

85. Payment by way of third party cheque or money transfer where there is variation between the account holder, the signatory and the prospective investor or where the payment information is unusual in relation to the domicile or residence of the investor.

86. Any request to make redemption settlement to a third party without any apparent connection with the investor.

Disposition

87. Settlement either by registration or delivery of securities to an unverified third party.

88. Abnormal settlement instructions including payment to apparently unconnected parties.

Reporting

89. A Fund as well as an FSP may have their own respective MLRO. For the avoidance of doubt, the MLRO of the Fund, where appointed, is responsible for suspicious activity reporting on behalf of the Fund, the FSP as a Designated Person has its own responsibilities in this regard. It is recommended that reporting and notification processes should be agreed between the FSP MLRO and the Fund MLRO including escalation of suspicious transactions (in the absence of tipping off concerns).

90. It should be noted that the Acts require that each Designated Person should report to the Garda Síochána and the Revenue Commissioners their suspicions of money laundering. If an arrangement is proposed where, for example to avoid duplication of reporting, *either* the FSP *or* the Fund reports to Garda Síochána and the Revenue Commissioners, this would need to be preapproved by the Garda Síochána and the Revenue Commissioners.

91. Until a decision has been made by the Fund or the FSP's Money Laundering Reporting Officer to notify the Gardai and Revenue Commissioners, further transactions or activity in respect of that investor, whether of the same nature or different, must also be included in the report. Where the FSP's Money Laundering Reporting Officer determines that a report is required they should not proceed with any suspicious transaction or service connected with the report, or with a transaction or service the subject of the report, prior to sending of the report to the Garda Síochána and the Revenue Commissioners unless it is not practicable to delay or stop the transaction from proceeding or they believe that stopping the transaction may result in the other person suspecting that a report may or may have been made. The report must be made as soon as practicable after reasonable grounds for suspicion exist.

92. If the Fund / FSP MLRO decide not to make a report to the Gardai and Revenue Commissioners, the reasons for not doing so should be recorded and retained by the MLRO.

93. The Fund / FSP MLRO must maintain a suspicious transaction reporting procedure, which clearly outlines the protocol around making such a report, and the FSP's MLRO must be able to demonstrate that a process for the ongoing monitoring of investor accounts and transactions is in place.

94. This policy must include controls and procedures around "tipping off" the investor that such a report may be in progress or has been made.

11. RECORD KEEPING

95. Section VIII of the Core Guidelines gives specific requirements for Designated Persons to maintain records and these should be reviewed in detail.

96. The legislation requires maintenance of:

- **i.** Customer Due Diligence records.
- **ii.** Transaction records by Designated Persons.
- **iii.** Other records required to demonstrate compliance with legislation relating to internal systems, training, reporting, compliance management, etc.

97. Documentation and information relating to Customer Due Diligence should be kept by Designated Persons for at least five years after cessation of the business relationship.

98. Documents relating to transactions should be kept for at least

- **i.** five years after the date on which the fund ceases to provide any service to the customer concerned or
- **ii.** five years after the date of the final transaction with the customer.

99. Where a Designated Person has an agent, it should ensure that the agent complies with the record keeping obligations under the legislation. This principle would also apply where the record keeping is delegated in any way to a third party. A third party outside the State must comply with requirements at least equivalent to those of the Third Money Laundering Directive.

100. Section 55 (7) of the Acts notes that although it is not necessary to keep documents in original form, where other storage media are used, the documents should be capable of being reproduced in written form.

12. STAFF TRAINING

What is required?

101. Under section 54(6) of the Acts, Designated Persons are required to ensure that persons involved in the conduct of the Designated Person's business are instructed on the law relating to money laundering and terrorist financing. These persons include the directors, other officers and employees of the Designated Person. The Acts also require that these persons partake in ongoing training to help them follow internal Customer Due Diligence and other anti-money laundering procedures in addition to the ability to identify a transaction or other activity that may be related to money laundering or terrorist financing and that they be instructed on the actions to take in such circumstances.

Section IX of the Core Guidelines gives further details on the required staff training and should be reviewed in detail.

102. To ensure maximum effectiveness it is recommended that, where possible, this training should relate to the funds industry by including examples or case studies that pertain to the Designated Person as a service provider to funds. AML/CTF training materials should include up to date information on the practices of money launderers and terrorist financiers and on indications leading to the recognition of suspicious transactions. Para 256 of the Core Guidelines indicates that AML training should refer to Data Protection requirements and indicate how they are relevant to AML requirements.

103. Failure to provide appropriate training on money laundering and terrorist financing is an offence on the part of the Designated Person as an employer. Training will include details on the law. Training should be provided no less frequently than on an annual basis and may be executed in one or all of the following manners as relevant to the size, complexity and type of business of each Designated Person:

- **i.** formal instructor-led training;
- **ii.** induction training/orientation; or
- **iii.** the completion of computer based training or other online modules.

Attendance of training should be documented.

What should Designated Persons do?

Education and training programmes

104. Timing and content of training of staff will need to be adapted by each individual Designated Person for their own needs and according to the specific roles of the individual staff members. The following is recommended:

New Staff

105. The Designated Person will provide training to include the following:

- **i.** background to money laundering and terrorist financing;
- **ii.** commentary on the Directive and the Acts including information on offences and penalties arising for non-reporting and providing assistance to money launderers and terrorist financiers;
- **iii.** the requirement (and personal statutory obligation) to report any suspicious activities to the MLRO (or delegate in his/her absence) without 'tipping off' the relevant investor(s), the customer, colleagues or others;
- **iv.** factors that may give rise to suspicions and the procedures to be adopted when a transaction is deemed suspicious;
- **v.** the importance placed on the reporting of suspicions by the Designated Person;
- **vi.** details of the Designated Person's systems for ongoing monitoring of investors and their transactions and the role the individual staff member plays in the functioning of this system; and
- **vii.** details of the Designated Person's procedures for ensuring the law is adhered to.

Note: training should be provided as a priority to new staff members dealing with investors or their transactions (irrespective of seniority).

Customer/Investor Facing Staff

106. The Designated Person will provide training to include the following:

- **i.** background to money laundering and terrorist financing;
- **ii.** commentary on the Directive and the Acts including information on offences and penalties arising for non-reporting and providing assistance to money launderers and terrorist financiers;
- **iii.** transaction processing and verification procedures;
- **iv.** recognition of abnormal settlement, payment or delivery instructions;
- **v.** the requirement (and personal statutory obligation) to report any suspicious activities to the MLRO (or delegate in his/her absence) without 'tipping off' the relevant investor(s), the customer, colleagues or others;
- **vi.** factors that may give rise to suspicions and the procedures to be adopted when a transaction is deemed suspicious;
- **vii.** the importance placed on the reporting of suspicions by the Designated Person; and
- **viii.** details of the Designated Person's systems for ongoing monitoring of investors and their transactions and the role the individual staff member plays in the functioning of this system.

107. Customer/investor facing staff are the first point of contact with potential money launderers and terrorist financiers and their efforts are therefore vital to the Designated Person's strategy in the fight against money laundering and terrorist financing. They should be made aware of the Designated Person's policy for dealing with high-risk investors and the need for extra vigilance in these cases.

Others (not Customer/Investor Facing)

108. The Designated Person will provide training to include the following:

i. background to money laundering and terrorist financing;
ii. commentary on the Directive and the Acts including information on offences and penalties arising for non-reporting and providing assistance to money launderers and terrorist financiers;
iii. the requirement (and personal statutory obligation) to report any suspicious activities to the MLRO (or delegate in his/her absence) without 'tipping off' the relevant investor(s), the customer, colleagues or others;
iv. factors that may give rise to suspicions and the procedures to be adopted when a transaction is deemed suspicious;
v. the importance placed on the reporting of suspicions by the Designated Person; and
vi. details of the Designated Person's systems for ongoing monitoring of investors and their transactions and the role the individual staff member plays in the functioning of this system.

Note: a higher level of instruction covering all aspects of money laundering and terrorist financing procedures should be provided to those with the responsibility for supervising or managing staff.

109. Those members of staff who process the settlement of transactions should receive appropriate training in the processing and verification procedures and in the recognition of abnormal settlement, payment or delivery instructions. The identity of the investor and matching against the cheque or payment received in settlement is, for instance, a key process. Such staff should be made aware that the offer of monies which are deemed suspicious, when undertaking an investment may need to be reported to the relevant authorities whether or not the funds are accepted or the transactions proceeded with. Staff should know the correct procedures to follow in this instance.

Nominated Reporting Officers/Money Laundering Reporting Officers

110. In nominating a Reporting Officer/Money Laundering Reporting Officer, a Designated Person should ensure that these officers have the requisite experience and/or training to fulfill their duties. Training concerning all aspects of the Acts and internal policies will be required for these officers.

Refresher Training/Ongoing Training

111. It will also be necessary to make arrangements for refresher training to ensure that staff (and in particular customer/investor facing staff) do not forget their responsibilities. While a Designated Person may wish to take a flexible approach to such training depending on their type of business, it is recommended that such training should take place no less frequently than on an annual basis.

Staff Awareness of Suspicious Activity

112. Sufficient training will need to be given to all relevant staff to enable them to recognise when a transaction or behaviour is unusual or suspicious, or when they should have reasonable grounds to know or suspect that money laundering or terrorist financing is taking place. The circumstances giving rise to an unusual transaction or arrangement, and which may provide reasonable grounds for concluding that it is suspicious, will depend on the investor and the product or service in question. Examples of the type of situation that may be unusual, and which in certain circumstances might give rise to reasonable grounds for suspicion in accordance with a Designated Person's risk based approach include:

i. Activities which have no apparent purpose, or which make no obvious economic sense (including where a person makes an unusual loss), or which involve apparently unnecessary complexity.

ii. The use of non-resident accounts, companies or structures in circumstances where the investor's needs do not appear to support such economic requirements.

iii. Where the activities being undertaken by the investor, or the size or pattern of transactions, are, without reasonable explanation, out of the ordinary range of services normally requested or are inconsistent with the experience of the Designated Person in relation to the particular investor.

113. Issues around the investor identification process that may raise concerns include such matters as the following:

i. Has the investor refused, or appeared particularly reluctant, to provide the information requested without reasonable explanation.

ii. Does the Designated Person understand the legal and corporate structure of the investor entity, and its ownership and control, and does the structure appear to make sense.

iii. Is the staff member aware of any inconsistencies between locations linked to the investor arising in the course of the business relationship and other information provided.

iv. Is the area of residence given consistent with other profile details, such as employment.

v. Does an address appear vague or unusual (e.g. an accommodation agency, a professional 'registered office' or a trading address).

vi. Does it make sense for the investor to be opening the account or relationship in the jurisdiction that he is asking for.

vii. Does the supporting documentation add validity to the other information provided by the investor.

viii. Does the investor want to conclude arrangements unusually urgently, against a promise to provide information at a later stage, which is not satisfactorily explained.

ix. Has the investor suggested changes to a proposed arrangement in order to avoid providing certain information.

114. It is important that staff are made aware of changing behavior and practices amongst money launderers and those financing terrorism. As well as their regular series of publications on the typologies of financial crime, FATF's Guidance Papers and Best Practices Papers contain in-depth analysis of the methods used in the financing of terrorism and the types of financial activities constituting potential indicators of such activities. These documents are available at www.fatf-gafi.org.

APPENDIX 1

Outlined below is general guidance on the documentation, which a Designated Person may request, when undertaking Standard Customer Due Diligence to prove the identity of an investor. We have prepared this guidance in the form of a matrix below, within the parameters of Lower Risk to Higher Risk and it is for each Designated Person to decide, within their risk-based assessment, the appropriate level and detail of documentation required to identify an investor within these parameters (refer to Section 6 'General Approach to Verification of Identity'.

It is unusual for Designated Persons to have face-to-face contact with fund investors. S33 (4) of the Acts details one or more additional measures which should be carried out' where a customer who is an individual does not present to the Designated Person for verification in person of the customer's identity'.

Examples of Standard Due Diligence –please refer to footnotes at the end of the matrix		
Investor Type[1]	**Standard Due Diligence-Lower Risk**	**Standard Due Diligence-Higher Risk**[2]
Individual Verify name, date of birth and address	**1.** A copy photographic identity document and a copy non-photographic identity document or **2.** The investor can be verified electronically. There are a number of products on the market which offer this e.g. Experian, ChoicePoint etc.	**1.** Certified[3] copy of a photographic identity document and two certified[3] or original non-photographic identity documents.
Joint Accounts/ Verify name, date of birth and address	Same as individuals except must be done for all parties.	Same as individuals except must be done for all parties.
Subsidiary of a company listed on a regulated market Identify corporate details, beneficial owners and directors / authorised signatories	**1.** Full name. **2.** Registered number. **3.** Registered office address. **4.** Principal business address. **5.** Identify directors (as per the documents referenced in point 7 below) **6.** Identify beneficial owners who own more than 25% of the share capital, profit or voting rights or otherwise exercise control over the management of the entity (confirm that entity is subsidiary of a company listed on a regulated market). **7.** Verification of identity from **i.** Search of the relevant company registry; and/or **ii.** Copy of Certificate of incorporation or equivalent; and/or **iii.** Copy of Memorandum and Articles of Association or equivalent; and/or **iv.** Copy of audited financial statements	**1.** Verify the identity[4]of two directors or one director and one authorised signatory. **2.** Verify the identity[4] of all beneficial owners beneficially entitled to more than 25% of the entity's share capital or voting rights of the entity or otherwise exercise control over the management of the entity

	8. Authorised signatory list.	
Private, unlisted companies and listed companies not qualifying for SCDD Verify corporate details, beneficial owners and directors / authorised signatories	Proof of listing, if appropriate. Full name. **1.** Registered number. **2.** Registered office address. **3.** Principal business address. **4.** Identify of directors. **5.** Verify the identity[4]of two directors or one director and one authorised signatory. **6.** Identify beneficial owners who own more than 25% of the share capital, profit or voting rights or otherwise exercise control over the management of the entity. **7.** Verification of identity from **i.** Search of the relevant company registry; and/or **ii.** Copy of Certificate of incorporation or equivalent; and/or **iii**. Copy of Memorandum and Articles of Association or equivalent; and/or **iv.** Copy of audited financial statements **8.** Authorised signatory list.	**1.** Verify the identity[4] of all beneficial owners beneficially entitled to more than 25% of the entity's share capital or voting rights of the entity. or otherwise exercise control over the management of the entity
Partnerships Verify partnership details and partners/ authorised signatories	**1.** Full name. **2.** Registered office address. **3.** Principal business address. **4.** Identify all partners (where not a Partnership Fund) or **5.** If a Partnership Fund, identify General Partner and partners who own more than 25% of the partnership capital, profit or voting rights or otherwise exercise control over the management of the entity and listing of directors, if appropriate. **6.** Verify the identity[4] of General Partner or two partners or one partner and one authorised signatory. **7.** Constitutional Document[4] (e.g. Partnership Agreement). **8.** Authorised signatory list.	**1.** Verify the identity[4] of all partners who own more that 25% of the partnership capital, profit or voting rights or otherwise exercise control over the management of the entity.
LLC/ Verify LLC details and members/ authorised signatories	**1.** Full name. **2.** Registered office address. **3.** Principal business address. **4.** identify Managing Members **5.** Verify the identity[4] of two Managing Members or one Managing Member and one authorised signatory. **6.** Identify Members who own more than 25% of the share capital, profit or voting rights or otherwise exercise control over the management of the entity. **7.** Constitutional Document[4] (e.g. Certificate of	**1.** Verify the identity[4] of all Members beneficially entitled to more than 25% of the entity's share capital or otherwise exercise control over the management of the entity.

	formation). **8.** Operating agreement. **9.** Authorised signatory list.	

Collective Investment Schemes not qualifying for SCDD Identify and verify CIS. Identify (and verify, if appropriate) all. beneficial owners of the CIS. May also obtain comfort on entity carrying out AML/CTF controls	If the scheme is listed in a regulated market then it may qualify for SCDD, otherwise the following documentation is suggested: **1.** Full name of CIS. **2.** Registered address of CIS. **3.** Prospectus[4] or equivalent **4.** Name and address of scheme promoter. **5.** Name and address of scheme administrator. **6.** Name and address of entity carrying out anti-money laundering checks upon the scheme investors and confirmation that entity is regulated for AML purposes. **7.** Names of all beneficial owners of the CIS. **8.** Authorised signatory list	**1.** Verify[4] all beneficial owners of the CIS. and/or **2.** Written confirmations from "responsible entity" i.e. the entity carrying out AML/CTF controls of CIS investors similar to that requested from relevant third parties undertaking due diligence; and/or **3.** Review of responsible entity's AML/CTF procedures; and/or **4.** Arrange for an independent due diligence review of responsible entity.
Trusts, foundations and similar entities Verify trust, trustees, settlor and beneficial owners **Note**: please see Section 5 of Appendix 1 of the Core Guidelines to ascertain where SCDD may apply to Trusts	**1.** Full name of trust. **2.** Registered address of trust. **3.** Consider legal form of the trust, foundation or similar entity **4.** Trust deed[4] or equivalent or confirmation of the entity to an appropriate register. **5.** Nature / purpose **6.** Identify all trustees **7.** Identify settlor **8.** Verify identity[4] of two trustees or one trustee and one authorised signatory. **9.** Identify all beneficial owners who own at least 25% of capital-.. –**please refer to Section IV of the core re the definition of 'Beneficial Owner' in relation to a trust** **10.** Authorised signatory list	**1.** Verify the identity[4] of any settlor, where practicable. **2.** Verify identity[4] of all beneficiaries who own at least 25% of the capital. –**please refer to Section IV of the core re the definition of 'Beneficial Owner' in relation to a trust.**
Pension Schemes not qualifying for SCDD Verify underlying employer and scheme	**1.** Full name **2.** Registered office address **3.** Authorised signatory list **4.** Confirmation of registration, as appropriate, from the relevant tax authorities or Pensions Board or obtain items 5, 6 and 7 below **5.** Identify Trustees/Directors/Governors /Board Members or equivalent **6.** Constitutional/Formation Document[4] (e.g. Trust Deed) **7.** Verification of two controllers – Trustees/Directors/Governors/Board Members or equivalent	**1.** Verify identity[4] of scheme administrator and entity carrying out AML/CTF controls on scheme investors, per legal form ; and/or **2.** Written confirmations from entity carrying out AML/CTF controls similar to that requested from third parties undertaking due diligence; and/or **3.** Review of responsible entity's AML/CTF procedures;

		and/or **4.** Arrange for an independent due diligence review of responsible entity
Charities Verify charity and selected officials/authorised signatories	**1.** Full name **2.** Nature/Purpose including the nature of the funding **3.** Registered office address **4.** Principal business address **5.** Authorised signatory list **6.** A check of a relevant Charities Register e.g. UK Charities Commission or obtain items 7-10 below **7.** Identify Trustees/Directors/Governors/Board Members or equivalent **8.** Verify the identity[4] of either two Trustees / Directors/ Governors / Board Members /equivalent, **or** one Trustee / Director/ Governor / Board Member/ equivalent, and one authorised signatory. **9.** Identify beneficiaries (where ascertainable) **10.** Constitutional/Formation Document[4]	**1.** Copy of audited financial statements.
Clubs and Societies Verify entity and selected officials/authorised signatories	Not applicable	**1.** Full name. **2.** Registered office address **3.** Nature/Purpose including the nature of the funding **4.** Confirmation of the legal status. **5.** Constitutional/Formation Document[4] (e.g. Trust Deed) and / or copy of audited financial statements (if available). **6.** Identify officers. **7.** Verification of the identity[4] of two of the officers of the Club/Society or one officer and one authorised signatory. **8.** Authorised signatory list.
Nominees and intermediaries not qualifying for SCDD (see section 8) Verify entity. Obtain comfort on AML/CTF controls operated	Where the Nominee Company is a wholly owned subsidiary of a regulated parent entity (in a Designated Country): **1.** Proof of regulation for the parent entity **2.** Letter from the regulated parent confirming: **a.** The parent company's home jurisdiction and its regulating authority.	**1.** Verify entity according to its legal form as a "higher risk" investor. and/or **2.** Obtain written confirmations from entity on AML/CTF controls similar to that requested from third parties undertaking due diligence; and/or

by entity.	**b.** That the Nominee is a wholly owned subsidiary and that it applies the AML policy of its parent entity.	**3.** Review of entity's AML/CTF procedures; and/or **4.** Arrange for an independent due diligence review of entity.

Credit or financial institutions to which SCDD does not apply Verify credit or financial institution details	**1**. Verify entity according to its legal form e.g. Private corporation, Partnership etc as a "lower risk" investor.	**1**. Verify entity according to its legal form e.g. Private corporation, Partnership etc as a "higher risk" investor".
Public bodies to which SCDD does not apply Verify public body details and officials	**1.** Full name. **2.** Nature and status **3.** Registered office address **4.** Name of the home state authority and nature of its relationship with public body. **5.** Ownership of the entity. **6.** Names of main public body officials. **7.** Identify all persons who own or control over 25% of the entity's share capital or voting rights of the body or otherwise exercises control over the management of the body. **8.** Authorised signatory list. **9.** Appropriate background information e.g. via internet search.	**1.** Verify the identity[4] of two officials or one official and one authorised signatory, where applicable and/or. **2.** Verify the identity[4] of all persons who own or control over 25% of the entity's share capital or voting rights of the body or otherwise exercises control over the management of the body, where applicable. **3.** Copy audited financial statements.
Schools, colleges or universities Verify entity details and officials	Schools, colleges or universities under State control should be treated as similar to public bodies; if the entity is independent then this may increase emphasis on independent background information. **1.** Full name. **2.** Registered office address. **3.** Authorised signatory list. **4.** Verify identity by checking with relevant registers and /or obtaining appropriate background information e.g. via internet search **5.** Verify the identity[4] of two officials or one official and one authorised signatory or obtain 6 and 7 below **6.** Determine the ownership of the entity. In particular, determine if owned publicly or privately. In case of the latter, identify all beneficiaries holding 25% or more of the assets. **7.** Obtain names of main officials.	**1.** Verify the identity[4] of all persons who own or control over 25% of the entity's share capital, profit or voting rights, where applicable.

[1:] Refer to Appendix 1 of the Core Guidelines for further details of documentation required.
[2:] The higher risk section details documents and actions, which are recommended to be obtained or performed *in addition* to those recommended in the lower risk section.

[3:] In terms of certified documents, this means that there is an original signature on the document from a suitable person. Suitable persons include:

- **Garda Siochana/Police Officers;**
- **Practicing Chartered & Certified Public Accountants;**
- **Notaries Public/Practising Solicitors;**
- **Embassy Consular Staff;**
- **Justice of the peace**
- **Commissioner for oaths**
- **Medical Professional**
- **Designated Persons as defined**
- **Designated Persons may determine that other persons with equivalent status to the persons in this list in the relevant jurisdictions might be suitable to certify and should document their reasons for this determination**

[4:] Identity should be verified according to your risk assessment. A Designated Person may decide as part of their risk-based approach that some documents should be received in original or certified form (see note 3 above), rather than just copies e.g. for a certain investor type or for individuals/entities based in certain jurisdictions.

APPENDIX 2

COMMON UNDERSTANDING

between Member States on third country equivalence[12]

under the Anti-Money Laundering Directive (Directive 2005/60/EC)

June 2012

These third countries are currently considered as having equivalent AML/CFT systems to the EU. **The list may be reviewed**, in particular in the light of public evaluation reports adopted by the FATF, FSRBs, the IMF or the World Bank according to the revised 2003 FATF Recommendations and Methodology.

It should be noted that the list does not override the need to continue to operate the risk-based approach. The fact that a financial institution is based in a 3rd country featuring on the list only constitutes a refutable presumption of the application of simplified CDD. Moreover, the list does not override the obligation under article 13 of the Directive to apply enhanced customer due diligence measures in all situations which by their nature can present a higher risk of money laundering or terrorist financing, when dealing with credit and financial institutions, as customers, based in an equivalent jurisdiction.

List after the Meeting on 26 June 2012

Australia	South Korea
Brazil	Mexico
Canada	Singapore
Hong Kong	Switzerland
India	South Africa
Japan	The United States of America

[1] Directive 2005/60/EC does not grant the European Commission a mandate to establish a positive list of equivalent third countries. The Common Understanding between EU Member States on Third Country Equivalence is drafted, managed and agreed by the EU Member States.

[2] The list does not apply to Member States of the EU/EEA which benefit de jure from mutual recognition through the implementation of the 3rd AML Directive. The list also includes the French overseas territories (Mayotte, New Caledonia, French Polynesia, Saint Pierre and Miquelon and Wallis and Futuna) and Aruba, Curacao, Sint Maarten, Bonaire, Sint Eustatius and Saba. Those countries and territories are not members of the EU/EEA but are part of the membership of France and the Kingdom of the Netherlands of the FATF. The UK Crown Dependencies (Jersey, Guernsey, Isle of Man) may also be considered as equivalent by Member States.

APPENDIX 3

Examples of Nominee and Intermediary Investments and possible approaches to CDD

FSPs should risk-assess and document due diligence measures to be taken in relation to all nominee or intermediary introductions; additional measures may need to be taken on the basis of the documented risk-assessment; these may include obtaining information and documentation, as applicable, on the underlying client of the nominee / intermediary.

a. A regulated entity in a designated country (which comes within the definition of 'Specified Customer' as set out in section 34 (5) of the Acts and Article 11 of the Directive) is the name on the Share Register of the Fund. The money is being invested either on behalf of the regulated entity or perhaps, on behalf of an underlying investor or group of investors under a discretionary investment management or similar arrangement. The regulated entity has full discretion and control over the monies being invested. E.g. ABC Bank Limited In this case SCDD will apply as the customer meets the definition of a 'Specified Customer'.

b. As per a. above except the regulated entity also references either an account number or account name in its naming on the register, for its own internal identification purposes. E.g. ABC Bank Limited a/c 12345 or ABC Bank Limited fbo John Smith.

c. A Nominee company of a regulated entity which is in a designated country is the name on the Share Register of the Fund. The regulated entity comes within the definition of 'Specified Customer' as set out in section 34 (5) of the Acts and Article 11 of the Directive. The Nominee Company is a wholly owned subsidiary of the regulated entity. The money is being invested at the direction of the regulated parent entity on its behalf or on behalf of its underlying investors or group of investors. The Nominee is considered to be a mere extension of the regulated entity and is the means through which the shares are obtained. The Nominee Company itself is not a regulated entity and may or may not be located in a designated country. E.g. ABC Nominees Limited. In this case, Standard Due Diligence will apply with confirmation from the regulated parent entity that the Nominee is a wholly owned subsidiary and applies the parent's AML policy.

d. As per c. above except that the Nominee references either an account number or account name in its naming on the register, for its own internal identification purposes. E.g. ABC Nominees Limited a/c 12345 or ABC Nominees Limited fbo John Smith. In this case, Standard Due Diligence will apply with confirmation from the regulated parent entity that the Nominee is a wholly owned subsidiary and applies the parent's AML policy.

e. A Nominee company of an unregulated entity is the name on the Share Register of the Fund and it is not related to an entity coming within the definition of Specified Customer set out in section 34 (5) of the Acts and Article 11 of the Directive. In this case Customer Due Diligence will apply at the appropriate level as per the risk assessed.