ISLE OF MAN
FINANCIAL SERVICES AUTHORITY

Lught-Reill Shirveishyn Argidoil Ellan Vannin

Customer Due Diligence

AML/CFT Guidance notes

October 2019

Whilst this publication has been prepared by the Financial Services Authority, it is not a legal document and should not be relied upon in respect of points of law. Reference for that purpose should be made to the appropriate statutory provisions.

Contact:
AML Unit, Enforcement Division
Financial Services Authority
PO Box 58,
Finch Hill House,
Bucks Road,
Douglas
Isle of Man
IM99 1DT
Tel: 01624 646000 Email: aml@iomfsa.im
Website: www.iomfsa.im

Version 01
(First issued October 2019)

Contents

1. Forward 4
2. Introduction 4
2.1. Definitions 4
2.2. Background to CDD 6
3. Key Principles of CDD 6
3.1. Cumulative approach 6
3.2. Foreign documents 6
3.3. Sanctions 7
3.4. Document verification and certification 7
3.5. Photographs and signatures 7
3.6. Signatories and attorneys 7
3.7. Doubts over information or documentation 7
3.8. Unable to obtain satisfactory CDD 8
3.9. Reporting suspicions 8
4. Code requirements 8
4.1. Minimum standards table 8
4.2. New business relationships and occasional transactions 10
4.3. Continuing business relationships 10
4.4. Beneficial ownership and control 12
4.5. Enhanced due diligence 18
5. Timing of ID&V and failure to complete ID&V 19
5.1. Timing in relation to continuing business relationships 20
6. How to “identify” 21
6.1 Natural persons 21
6.2. Legal persons 21
6.3. Legal arrangements 22
7. What to “verify” 22
7.1. Natural persons 23
7.2. Legal persons 23
7.3. Legal arrangements 23
7.4. ID&V requirements for multiple signatories/directors 24

7.5. ID&V requirements for multiple 3rd parties 25
7.6. ID&V requirements for clubs and associations 25
8. Methods to verify natural persons 26
8.1. Acceptable methods to verify identity 27
8.2. Acceptable methods to verify address 28
8.2.1. Change of address 28
9. Methods to verify legal persons 33
10. Methods to verify legal arrangements 35
11. Certification of hard copy documents 37
12. Use of electronic documents 38
13. Independent electronic data sources 39
14. Purpose and intended nature of business relationship 39
15. Source of funds and source of wealth 40
16. Bearer shares 40
17. Politically Exposed Persons ("PEPs") 41
17.1. PEP risk 41
17.2. PEP definitions 41
17.3. PEP requirements 43
17.4. Identifying PEPs 45
17.5. Identifying PEP risk 46
17.6. "Once a PEP, always a PEP"? 47

1. Forward

This document is issued to cover the period whilst the Anti-Money Laundering & Countering the Financing of Terrorism Handbook ('the Handbook') is being updated. When the new Handbook is published the information contained in the document will be amalgamated into the main body. The Handbook contains guidance on all other areas of the Anti-Money Laundering and Countering the Financing of Terrorism Code 2019 ("the Code").

2. Introduction

2.1. Definitions

For ease of reference some of the key terms from this part of the Handbook are explained in this introductory section.

Customer Due Diligence ("CDD")

CDD involves obtaining, documenting and using a broad range of information relating to a customer relationship or an occasional transaction. Areas to be considered include identity, address, source of funds and expected business or transactional activity. Certain elements of this information must also be verified. The term CDD also incorporates the ongoing monitoring of a business relationship, including the due diligence information obtained, to ensure it remains up to date and that the relationship is operating as expected for that customer. CDD is required for all new or continuing business relationships or occasional transactions.

Identification and Verification ("ID&V")

ID&V is essentially the concept of the relevant person satisfying itself that their customer is who they say they are. ID&V falls within CDD and specifically refers to obtaining information concerning a customer's identity and the verification of that customer's identity. Verification in this context refers to verifying elements of identification information by using independent reliable sources; such sources may include material obtained from the customer, such as a passport to verify the customer's name. A relevant person must ensure, through the checks undertaken, that they are satisfied the customer is who they say they are. Most importantly, the relevant person must be satisfied they are in compliance with the Code requirements at all times.

The following part of the Handbook provides information in relation to how to go about identifying, and verifying the identity, of a customer. It includes best practice guidelines in relation to components of identity that relevant persons should obtain information about, and subsequently verify, where appropriate, in order to meet their obligations under the Code. Exactly what information is actually obtained (and subsequently verified) will vary on a case to case basis as in relation to some customers not all of the components may be able to be obtained, or verified.

The expectations of the Authority are that best endeavours are taken to use the methods outlined in this section, however there is the option to obtain senior management sign off if the information and documentation obtained varies from suggested best practice included in this Guidance.

Enhanced Customer Due Diligence ("EDD")

EDD goes further than obtaining CDD. This involves:

- considering whether additional identification information needs to be obtained (and obtaining this information):
- considering whether additional verification of identity is required (and obtaining this additional verification):
- taking reasonable measures to establish source of wealth (in addition to establishing the source of funds) of the customer and beneficial owner;
- undertaking further research, where considered necessary, in order to understand the background of a customer and the customer's business; and
- considering what additional ongoing monitoring of this information should be undertaken, including of CDD and ECDD information.

EDD is to be undertaken when a new business relationship, occasional transaction, or a continuing business relationship is assessed as posing a higher risk of ML/FT, or when unusual activity is identified. When suspicious activity is detected EDD must be undertaken, unless the relevant person believes conducting EDD will tip off the customer (as well as making an internal disclosure).

Enhanced Monitoring

Enhanced monitoring should examine all aspects of the business relationship including the CDD / any EDD already obtained and the customer's activity. In particular it should focus on any changes in transactions or activity, and in particular any transactions or activity that is not in line with the customer's expected activity.

These transactions and activities should be scrutinised more thoroughly. Appropriate screening for negative press should also be undertaken as well as further open source internet searches undertaken as necessary.

In relation to any foreign PEPs, and higher risk domestic PEPs, the Code requires that enhanced monitoring is undertaken of the business relationship. The Authority would expect enhanced monitoring of these particular categories of PEPs to take place at least annually.

2.2. Background to CDD

CDD is defined in the Code as meaning the measures specified in Paragraphs 8 to 14, 16 to 22, 36, 37 and 39 of the Code. The CDD requirements apply at the outset of a business relationship or occasional transaction (as per paragraphs 8 and 11 of the Code). They also apply in relation to continuing business relationships (paragraph 10 of the Code). In certain circumstances EDD may be required, EDD is explained further in section 4.5.

Robust CDD procedures are vital for all relevant persons because they:

- help protect the relevant person and the integrity of the Isle of Man financial and designated business sectors by reducing the likelihood of relevant persons becoming a vehicle for, or victim of, financial crime;
- assist law enforcement by providing available information on customers or activities, funds or transactions being investigated;
- constitute an essential part of sound risk management e.g. by providing the basis for identifying, limiting and controlling risk exposures; and
- help to guard against identity theft.

Inadequate CDD standards and controls can result in serious customer and counterparty risks for relevant persons. Particularly in relation to reputational, operational, legal and concentration risks, which can result in significant financial cost to the business and potentially legal action being taken against the relevant person.

CDD information is also a vital tool for relevant persons to aid in the recognition of unusual or suspicious activity, therefore the CDD information held should be utilised when monitoring activity of business relationships and transactions. The ongoing monitoring requirements are explained further in paragraph 13 of the Code and part 3.4 of the Handbook.

3. Key Principles of CDD

3.1. Cumulative approach

CDD is generally a cumulative process with more than one document or data source being required to verify relevant components. The extent of documentation and information which is required to be collected varies depending on the customer's risk rating. Relevant persons will need to be prepared to accept a range of documents and data. However, relevant persons should be aware that some documents are more easily forged than others.

3.2. Foreign documents

Relevant persons should ensure that any key documents obtained as part of the CDD process which are in a foreign language are adequately translated into English. This is to ensure the true significance of the document can be appreciated. This should be considered on a case by case basis as it may be obvious in certain instances what a document is and what it means, however in other cases it may not. If the decision is made not to translate a foreign document the relevant person should document why it

has not been translated and include a summary of what they believe the document is. This should be appropriately signed off by a staff member of appropriate seniority.

Where customers put forward documents with which the relevant person is unfamiliar, either because of origin, format or language, the relevant person should take reasonable steps to verify that the document is indeed genuine. This may include contacting the relevant authorities. Consideration should be given to the importance of the detail of the document. If a translation is made a copy of the translation of the document should be obtained and kept with the original or copy document as evidence.

3.3. Sanctions

Relevant persons should check a customer's (including beneficial owners and controllers where appropriate) nationality, residency, expected activities and source of funds to ensure that they are not subject to any relevant financial sanctions at the outset of the relationship but also on an ongoing basis. More information on sanctions can be found within part 7 of the Handbook.

3.4. Document verification and certification

Where CDD documentation is obtained in hard copy, this must be certified by a suitable certifier. For identity documents the certifier must have seen the original document and met the individual. Where CDD documentation is obtained electronically the authenticity of this document must be appropriately verified.

3.5. Photographs and signatures

Any photocopies showing photographs and signatures should be clearly legible. In face-to-face situations, relevant persons should check that the photograph represents a good likeness of the customer.

3.6. Signatories and attorneys

In circumstances where a customer appoints another person as an account signatory e.g. an expatriate appointing a member of his family, or company directors appointing a non-director as a signatory, or granting power of attorney in favour of an individual, full CDD procedures should also be carried out on the new account signatory or attorney. Further information can be found at paragraphs 7.4 and 7.5 of this document.

3.7. Doubts over information or documentation

Irrespective of the type of business relationship or transaction, or whether the customer is a natural or legal person, where any doubt arises as to the CDD information or verification of that information, this constitutes unusual activity. In this case the relevant person must undertake EDD and perform appropriate scrutiny of the activity unless the relevant person believes conducting EDD will tip off the customer. The relevant person must also consider whether an internal disclosure is appropriate. Further information regarding unusual/suspicious activity can be found at part 7 of the Handbook.

3.8. Unable to obtain satisfactory CDD

Where any of the customer's information or documentation cannot be obtained, and where necessary verified, to a satisfactory standard that is sufficient to comply with the Code the following steps must be taken:

- the business relationship or transaction must proceed no further;
- the business relationship must be terminated; and
- the relevant person must consider making an internal disclosure.

In circumstances where this is the case, all information and documentation that has been obtained should be retained for at least 5 years from the relevant date. Further information regarding reporting requirements can be found at part 7 of the Handbook and the record keeping provisions are explained at part 8 of the Handbook.

3.9. Reporting suspicions

Where a relevant person identifies any suspicious activity, or has reasonable cause to suspect ML/FT by a prospective customer and the business relationship has not proceeded, an internal disclosure must be made. The requirement is irrespective of the type of prospective customer. Further information regarding reporting requirements can be found at part 7 of the Handbook.

4. Code requirements

Relevant persons should apply a graduated customer acceptance policy which requires EDD to be undertaken on those customers who are assessed as representing a higher risk of ML/FT. However, even when a customer is considered to represent a lower risk of ML/FT, the minimum standard of CDD procedures in the Handbook should be applied. As explained above, alternative methods of CDD not included in this guidance can be used, however senior management approval should be obtained in these circumstances.

Part 6 of the Handbook provides further detail on other Simplified CDD Measures which may be permitted in certain circumstances.

There are additional Code requirements for any customer who is a Foreign PEP (regardless of risk rating), or a domestic PEP who has been identified as posing a higher risk of ML/FT. Information regarding the Code requirements for PEPs and how to identify them is at section 17 of this document.

4.1. Minimum standards table

The table overleaf is intended to provide a very high level summary of the minimum CDD requirements depending on the risk category of customer. It should be used in conjunction with the relevant parts of this document and the Handbook which cover this in greater detail.

	Lower and Standard Risk (CDD)	**Higher Risk** **(EDD)** (as per Code para 15)	**Foreign PEPs & Higher Risk Domestic PEPs** (as per Code para 14 in addition to EDD where applicable)
Identification information (Customer)	Required before or during the formation of the relationship	Consider additional information and verification in addition to standard CDD requirements. As well as further research where considered necessary, in order to understand the background of a customer and their business.	As per standard or higher risk as determined by risk rating.
Verification of that information (Customer)	May be undertaken following the establishment of the business relationship in **very limited circumstances**		
Identification information (Underlying customer, persons acting on behalf of, beneficial owners)	Required before or during the formation of the relationship		
Verification of that information (Underlying customer, persons acting on behalf of, beneficial owners, legal status)	Reasonable measures May be undertaken following the establishment of the business relationship in **very limited circumstances**		
Purpose / intended nature of relationship	Required before or during the formation of the relationship	Required before or during the formation of the relationship	
Source of Funds	Reasonable measures to establish	Reasonable measures to establish	
Source of Wealth	No legislative requirement – best practice only	Reasonable measures to establish	Reasonable measures to establish
Obtain senior management approval to take on business	No legislative requirement	No legislative requirement	Required before relationship is established
Ongoing monitoring	Ongoing and effective monitoring	Ongoing and effective monitoring, also consider additional ongoing monitoring	Must perform ongoing and effective enhanced monitoring

4.2. New business relationships and occasional transactions

Paragraphs 8 and 11 of the Code require the relevant person to establish, record, maintain and operate procedures and controls in respect of new customers or occasional transactions which cover the following:

(a) identifying the customer;
(b) verifying the identity of the customer using reliable, independent source documents, data or information;
(c) verifying the legal status of the customer using reliable, independent source documents, data or information;
(d) obtaining information on the nature and intended purpose of the business relationship; and
(e) take reasonable measures to establish the source of funds, including whether the funds are received from an account not in the name of the customer
    (i) understanding and recording the reasons for this;
    (ii) identifying the account holder and on the basis of materiality and risk of ML/FT taking reasonable measures to verify the identity of the account holder using reliable, independent source documents, data or information; and
    (iii) if the account holder is assessed as posing a higher risk of ML/FT, satisfying the requirements in paragraph 15

Consideration should be given to additional procedures, explained later in document where the customer is assessed as posing a higher risk, is a foreign PEP or a higher risk domestic PEP.

All CDD procedures must be undertaken before, or during the formation of, the relationship. In exceptional circumstances only, the verification of identity may be undertaken following the formation of that relationship provided that certain conditions are met, see section 5 of this document for further details relating to this concession.

Please see Part 6 of the Handbook for details of “exempted occasional transactions” to which certain requirements of paragraph 11 of the Code may not apply in certain circumstances.

4.3. Continuing business relationships

Paragraph 10 of the Code requires the relevant person to establish, record, maintain and operate procedures in respect of continuing business relationships (existing relationships established prior to the 2019 Code) including:

(a) an examination of the background and purpose of the business relationship;
(b) if satisfactory verification of the customer's identity was not obtained or produced, requiring such verification to be obtained or produced in accordance with paragraph 8;
(c) if satisfactory verification of a customer's identity was obtained or produced, a determination as to whether it is satisfactory; and
(d) if the verification of identity is not satisfactory for any reason, requiring that the relevant person takes measures to verify the customer's identity in accordance with paragraph 8.

Continuing business covers the scenario where new Code requirements are introduced for existing sectors already subject to the Code requirements, and also includes any business relationships held prior to AML/CFT requirements coming in for a particular business sector. It is anticipated this will only affect a small number of relevant persons.

The requirements at paragraph 10 of the Code must be undertaken during a business relationship as soon as reasonably practicable

As per paragraph 10, if verification of identity has not already been obtained, or that which was obtained is unsatisfactory (for example, because the verification requirements have been changed / enhanced since the original verification of identity was obtained), relevant persons must take steps to obtain satisfactory verification of identity. Where verification of identity documentation obtained previously has subsequently expired a relevant person does not automatically have to update this documentation.

Ongoing Monitoring provisions at Paragraph 13 of the Code:

The ongoing monitoring requirements for customers where satisfactory CDD was undertaken at the outset of the business relationship or transaction are explained in paragraph 13 of the Code. See part 3 of the Handbook for further details regarding to ongoing monitoring of business relationships.

For these continuing relationships, whether CDD needs to be undertaken will depend upon whether the relevant person already obtained the relevant information and documentation at the beginning or during the course of the relationship previously and whether, if it has been obtained, it is satisfactory and complies with current standards.

Relevant persons will therefore need to examine the information and documentation they already hold to determine whether it is necessary to collect additional CDD or make further enquiries either from the customer concerned or from other sources. If during this review it is identified that CDD needs to be renewed as it is not up-to-date and/or appropriate, the procedures under paragraph 10 of the Code should be used.

4.4. Beneficial ownership and control

Paragraph 3 of the Code defines beneficial owner as:

> the natural person who ultimately owns or controls the customer or on whose behalf a transaction or activity is being conducted and includes but is not restricted to:
>
> (a) in the case of a legal person other than a company whose securities are listed on a recognised stock exchange, a natural person who ultimately owns or controls (whether through direct or indirect ownership or control, including through bearer share holdings) 25% or more of the shares or voting rights in the legal person;
> (b) in the case of any legal person, a natural person who otherwise exercises ultimate effective control or significant influence over the management of the legal person;
> (c) in the case of a legal arrangement, the trustee or other person who exercises ultimate effective control or significant influence over the legal arrangement; and
> (d) in the case of a foundation, a natural person who otherwise exercises ultimate effective control or significant influence over the foundation;

Please note that the definition of beneficial owner in the Code differs from the definitions in the Beneficial Ownership Act 2017 and the Insurance Act 2008. The Beneficial Ownership Act 2017 can be found here. The Authority has issued guidance regarding the Beneficial Ownership Act 2017, which can be found here.

This part of the document further explains some of the persons associated with the customer that should be identified and their identity verified where necessary. A relevant person must be satisfied it knows who the beneficial owner of its customer is. Therefore where a person identified is not an individual, it would be necessary to look through to the natural person(s) that ultimately owns or exercises ultimate effective control or significant influence of the customer.

The relevant person should consider whether any persons associated with the customer that need to be ID&Vd would result in a higher risk rating for that customer. This in turn may impact on the appropriateness of utilising any simplified CDD measures for the customer and any associated persons as explained in part 6 of the Handbook.

Where there is a change in any of the parties who are acting on behalf of a customer or there is a change in beneficial ownership and control of a customer, relevant

persons should treat these persons as new relationships and CDD requirements must be applied as required by paragraphs 8 and 11 of the Code.

Paragraph 12(2)(a) of the Code requires that where a customer is not a natural person the relevant person must –

> (i) identify who is the beneficial owner of the customer, through any number of persons or arrangements of any description; and
>
> (ii) subject to paragraphs 11(4), 11(5), 16(2) and 18(2) take reasonable measures to verify the identity of any beneficial owner of the customer, using reliable, independent source documents, data or information;

Paragraph 12(2)(b) of the Code is relevant for any customer. It requires a relevant person to:

> subject to paragraphs 17 and 21, determine whether the customer is acting on behalf of another person and, if so —
>
> (i) identify that other person; and
>
> (ii) take reasonable measures to verify that other person's identity using reliable, independent source documents, data or information;

This is intended to ensure that any persons who your customer is acting for, or on behalf of, are appropriately ID&Vd.

A relevant person must assess each business relationship on a case by case basis to determine if the customer is acting for another person ("an underlying client"). It is also necessary to determine whether the underlying client exercises control over the relationship, or whether the relationship is operating through a third party. When assessing this the relevant person could consider matters such as:

- do instructions come from the customer/the customer's signatories? Or do they show evidence of being from an underlying client, countersigned by the customer?
- the immediate source of funds;
- the destination of funds i.e. are the funds being remitted to the underlying client or to a third party;
- does the account title indicate that there are underlying clients?
- payment references or rationale that does not appear to relate to the purported customer; and

- whether it appears that the customer has had to refer to underlying clients to obtain information.

If the assessment of the relationship indicates that the underlying client exercises control over the relationship; however, a third party is acting on the underlying client's behalf, in addition to identifying and verifying the customer a relevant person must also identify and verify the identity of the underlying client. This is subject to certain simplified CDD concessions detailed in Part 6 of the Handbook which permit the third party to be treated as the customer provided that relevant conditions are met (see Paragraph 17 of the Code).

If a relevant person determines that there is no underlying client, or that the underlying client does not control the relationship, then the customer would not be considered as acting on behalf of another person and should be taken on in the usual manner under part 4 of the Code.

Relevant persons must satisfy themselves and document the outcome in relation to establishing for each business relationship, who the customer is, whether they are acting for another person, and what CDD is required.

Legal Arrangements

In the case of a legal arrangement, paragraph 12(3) requires a relevant person to, identify and take reasonable measures to verify the identity of the beneficial owner -

> (a) in the case of an express trust, by identifying —
>
> (i) the trustees or any other controlling party;
>
> (ii) any known beneficiaries;
>
> (iii) any class of beneficiaries and, in respect of a class of beneficiaries where it is not reasonably practicable to identify each beneficiary details sufficient to identify and describe the class of persons who are beneficiaries;
> (iv) the protector (if any);
>
> (v) the enforcer (if any);
>
> (vi) the settlor, or other person by whom the legal arrangement is made or on whose instructions the legal arrangement is formed; and
>
> (vii) any other natural person exercising ultimate effective control over the trust traced through any number of persons or arrangements of any description; and

(b) in the case of other types of legal arrangement by identifying any natural persons in equivalent or similar positions to those mentioned in head (a), traced through any number of persons or arrangements of any description.

This includes protectors (or similar), co-trustees or other third parties (including the settlor) where significant powers are retained or delegated. Where a blind trust or dummy settlor is used, this places an obligation on the relevant person to identify the individual who gave the instructions to form the legal arrangement and any person funding the establishment of the arrangement.

Relevant persons should also obtain information regarding classes of beneficiaries to enable them to have the capacity to determine the identity of a beneficiary in future and appropriately risk assess the relationship. If it is not reasonably practicable to identify each beneficiary details sufficient to identify and describe the class of persons who are beneficiaries.

Foundations

In the case of a foundation, paragraph 12(4) requires a relevant person to, identify and take reasonable measures to verify the identity of the beneficial owner by identifying –

(a) the council members (or equivalent);

(b) any known beneficiaries;

(c) any class of beneficiaries, and in respect of a class of beneficiaries where it is not reasonably practicable to identify each beneficiary, details sufficient to identify and describe the class of persons who are beneficiaries;

(d) the founder and any other dedicator; and

(e) any other natural person exercising ultimate effective control over the foundation through any number of persons or arrangements of any description.

In respect of foundations, which are legal persons but which resemble trusts in many ways, relevant persons must identify the persons referred to above. It is also necessary to obtain identification information on any other person(s) with a sufficient interest, including a person who in the view of the High Court, can reasonably claim to speak on behalf of an object or purpose of the foundation and a person who the High Court determines to be a person with a sufficient interest under section 51(3) of the Foundations Act 2011 (or equivalent in non-Isle of Man established foundations).

Where a foundation council member who has been verified is replaced, the identity of the new council member must be verified before they are allowed to exercise any control over the assets.

Relevant persons should also obtain information regarding classes of beneficiaries to enable the relevant person to have the capacity to determine the beneficiary in the future and appropriately risk assess the relationship. If it is not reasonably practicable to identify each beneficiary details sufficient to identify and describe the class of persons who are beneficiaries.

Legal Persons

In the case of a legal person, paragraph 12(5) requires a relevant person to a relevant person must, identify and take reasonable measures to verify the identity of the beneficial owner by –

> (a) obtaining the identity of the beneficial owner who ultimately has a controlling interest in the legal person;
>
> (b) if it is not possible to comply with head (a) or where no natural person is the ultimate beneficial owner, identifying and taking reasonable measures to verify the identity of any natural person who exercises control of the legal person; and
>
> (c) if it is not possible to comply with head (a) or (b), or where no natural person is the ultimate beneficial owner, identifying and taking reasonable measures to verify the identity of any natural person who exercises control of the legal person through other means, such as acting as a senior managing official.

This should be done by identifying the beneficial owner who ultimately has a controlling interest in the legal person. If there is no natural person identified as the ultimate beneficial owner, identifying and taking reasonable measures to verify the identity of any natural person who exercises control of the legal person. If the above cannot be complied with the relevant person should identify and taking reasonable measures to verify the identity of any natural person who exercises control of the legal person through any other means, such as senior managing official.

Legal Persons and Arrangements

In relation to both legal persons and arrangements, paragraph 12(6) requires a relevant person to -

> (a) obtain the name and address of any other natural person who has the power to direct the customer's activities and take reasonable measures to verify that information using reliable, independent source documents, data or information;

This is referring to persons exercising control over the management and having power to direct the activities of a customer that may not deemed to be a controller, or one

of the parties referred to above, such as any remaining directors, persons with Powers of Attorney or account signatories.

For legal persons not listed on a recognised stock exchange, this includes (but is not restricted to) any individual who ultimately owns or controls (whether directly or indirectly) 25% or more of the shares or voting rights in the legal person. For all legal persons this includes any individual who otherwise exercises control over the management of the legal person e.g. persons with less than 25% of the shares or voting rights but who nevertheless hold a controlling interest.

For a legal arrangement, this includes persons whose instructions or requests the trustees are accustomed to acting on, for the avoidance of doubt, this includes where those instructions are not binding.

Methods to verify this information may include obtaining a copy of signatory lists, the most recent annual return, third party authority signing mandate or a register of directors.

> (b) obtain information concerning the person by whom, and the method by which, binding obligations may be entered into or imposed on the customer; and

This includes taking reasonable measures to obtain information regarding the roles and powers of any persons as described above and obtaining copies of authority such as Memorandums and Articles of Associations, Power of Attorney, a signatory list plus a copy of a board resolution relating to the signatory list. The Authority expects a relevant person to take a risk based approach in this regard and consider verifying the identity of persons able to exercise a high level of control over the customer or where other high risk factors are present.

> (c) obtain information to understand the nature of the customer's business and the ownership and control structure of the customer.

This may include structure charts and lists detailing the persons as described above plus details of the group's structure and any connected entities as appropriate.

Paragraph 12(7) requires that –

> Subject to paragraph 21(1) and without limiting sub-paragraphs (2)-(6), the relevant person must not, in the case of a customer that is a legal person or a legal arrangement, make any payment or loan to, or on behalf of, a beneficial owner of that person or for the benefit of a beneficiary of that arrangement unless it has —

(a) identified the recipient or beneficiary of the payment or loan;

(b) on the basis of materiality and risk of ML/FT, verified the identity of the recipient or beneficiary using reliable, independent source documents, data or information; and

(c) understood the nature and purpose of that payment or loan in accordance with paragraph 13.

Where a payment such as a distribution or loan is made to an unconnected third party on behalf of a beneficiary or beneficial owner, that third party must be identified (the extent of identification information obtained by the relevant person could be determined on a risk based approach) and the relevant person must consider verifying the identity of this party on a risk based approach

For example, in the case of making a payment for a routine repair to a property or school fees, a check to satisfy yourself that a payee exists and appears to be legitimate would be sufficient. However, where a payment is being made to an unknown third party, more substantive checks should be undertaken.

The relevant person must be satisfied with the CDD obtained before making a payment to a third party. Instances include, but are not limited to:

- making a loan to a third party;
- repaying a liability or loan on behalf of a beneficiary or beneficial owner; or
- paying an invoice on behalf of a beneficiary or beneficial owner.

For the avoidance of doubt, this sub-paragraph applies to any type of payment including a partial revocation of a trust.

In relation to payments made in the case insurance policies see the relevant sector 7guidance issued for the life and non-life sectors.

4.5. Enhanced due diligence

In order to enable further scrutiny of a business relationship or an occasional transaction paragraph 15(3) of the Code states that EDD must be carried out in the following circumstances:

(a) where a customer poses a higher risk of ML/FT as assessed by the customer risk assessment;

(b) without limiting paragraph 13, in the event of any unusual activity; and

(c) without limiting paragraph 26, in the event of any suspicious activity, unless the relevant person reasonably believes conducting enhanced customer due diligence will tip off the customer.

EDD is defined in the Code as meaning steps additional to the measures detailed in paragraphs 8 to 14, 16 to 22, 36, 37 and 39 and consists of –

- considering whether additional identification information needs to be obtained (and obtaining this information);
- considering whether additional aspects of the identity need to be verified (and obtaining this additional verification);
- the taking of reasonable measures to establish source of wealth (in addition to source of funds) of the customer and any beneficial owner;
- undertaking further research, where considered necessary, in order to understand the background of a customer and the customer's business; and
- considering what additional on-going monitoring should be carried out.

In considering what EDD is appropriate, it is necessary to recognise that the information requirements for identifying and reporting suspected FT may be different from those for ML. ML involves the proceeds of crimes which have already taken place. FT may also involve the proceeds of crime, but equally it may involve completely clean funds. In FT situations, it is the destination of funds which is of primary importance as they may be used to finance future terrorist attacks, organisations, resources and support networks.

In undertaking EDD where there is a higher risk of FT, relevant persons should have particular regard to their customer's relationships and the destination of funds which will, or have, formed part of the relevant person's relationship with its customer.

It is necessary for relevant persons to document their deliberations and rationale when deciding what additional measures are required in order to demonstrate that the EDD requirements in the Code have been met.

EDD procedures for new customers that are assessed as posing a higher risk or ML/FT must be undertaken before or during the formation of that relationship. There is no concession to delay the timing of obtaining the identity information and verification of this.

5. Timing of ID&V and failure to complete ID&V

In respect of any new business relationships, or an occasional transaction, relevant persons must obtain CDD before a business relationship (or transaction) is entered into, or during the formation of that business relationship.

However, very exceptionally, where there is little risk of ML/FT occurring, the Code allows at paragraph 8(4) for the verification of identification to be carried out after the formation of a business relationship (this does not apply to an occasional transaction) provided that:

(a) it occurs as soon as reasonably practical;
(b) the delay is essential so as not to interrupt the normal course of business;
(c) the customer has not been identified as posing a higher risk of ML/FT;
(d) the risks of ML/FT are effectively managed;
(e) the relevant person has not identified any unusual activity or suspicious activity;
(f) the relevant person's senior management has approved the establishment of the business relationship and any subsequent activity until sub-paragraphs (3)(b) and (c) have been complied with;
(g) the relevant person ensures that the amount, type and number of transactions is appropriately limited and monitored.

An example of where this concession may be used is in relation to securities transactions where companies may be required to perform transactions very rapidly, according to the market conditions at the time that the customer is contacting them, and the performance of the transaction may be required before the verification of identity is completed.

Such procedures utilising this paragraph of the Code must include a set of measures such as a limitation on the number, types and/or amount of transactions that can be performed and the monitoring of large or complex transactions being carried out outside of norms for that type of relationship. As an absolute minimum we would not expect a relevant person to repay funds to the customer or a third party until the identification has been verified.

Relevant persons must satisfy themselves that the primary motive for the use of this concession is not for the circumvention of CDD procedures. The relevant person should document the justification for the use of this concession.

The CDD process (including the requirements of paragraphs 8, 11, 12, 14 and 15), once begun, should be pursued through to conclusion within a reasonable timeframe. If a prospective customer does not pursue an application, or verification cannot be concluded within a reasonable timeframe and without adequate explanation, the business relationship shall not proceed any further and the relevant person must terminate that relationship and consider whether an internal disclosure should be made.

5.1. Timing in relation to continuing business relationships

Paragraph 10 of the Code refers to the CDD requirements for continuing business relationships. Paragraph 10(3) of the Code requires that where satisfactory verification of identity was not obtained or produced, or is not satisfactory, the relevant person must take measures to verify the customer's identity in accordance with paragraph 8.

The satisfactory verification of identity should be undertaken a reasonable period of time. The Authority considers that this information should be obtained within 6 months of the legislation coming into effect. There may be flexibility on this time scale (such as where a business has a particularly large customer base and 6 months is impractical). Where such a decision is made on the grounds of impracticality, the rationale behind this should be documented and the Authority should be informed of the relevant person's proposed timetable to remediate this.

6. How to "identify"

6.1 Natural persons

In order to "identify" a natural person, the following identification information should be obtained:

(a) legal name, any former names (e.g. maiden name) and any other names used;
(b) permanent residential address (including post code if possible);
(c) date of birth;
(d) place of birth;
(e) nationality (including any other nationalities);
(f) gender;
(g) an official personal identification number or other unique identifiers contained in an un-expired official document; and
(h) identification information relating to any underlying customers or persons purporting to act on behalf of the customer.

The following may also be collected taking a risk-based approach:

(i) occupation and name of employer/source of income; and
(j) details of any public or high profile positions held.

6.2. Legal persons

In order to "identify" a legal person, the following identification information should be obtained:

(a) name of entity;
(b) type of legal person;
(c) any trading names;
(d) date and country of incorporation/registration/establishment;
(e) official identification number; (e.g. tax identification number or registered charity number);
(f) whether listed and if so, where;
(g) registered office address and in respect of foundations the business address;
(h) principal place of business/operations (if different from registered office);
(i) mailing address (if different from registered office);
(j) name of regulator (if applicable); and

(k) identification information on the underlying customer, any person purporting to act on behalf of the legal person and the beneficial owners of the legal person.

6.3. Legal arrangements

In order to "identify" a legal arrangement, the following identification information should be obtained:

(a) name of trust;
(b) date of establishment;
(c) official identification number where applicable (e.g. tax identification number or registered charity number);
(d) identification information for any related natural persons related to the legal arrangement including the beneficial owner, known beneficiaries, controlling parties including the trustee(s) or other persons controlling or having power to direct the activities of the customer in line with the guidance for natural and legal persons[1] (this includes protectors, co-trustees, or other third parties (including the settlor) where significant powers are retained or delegated; and
(e) mailing address(es) of trustee(s) or other persons controlling or having power to control the customer (as above);
(f)

7. What to "verify"

Whichever of the following methods is used for verifying identification information or address, in all cases, either an original document, electronic copy of a document or a certified copy of the relevant documentation should be retained on file to evidence that verification has been undertaken. Relevant persons should ensure they are comfortable with the authenticity of the document. For further information on record keeping see sections 11 and 12 of this document and 8.4 of the Handbook.

It should be noted that in some cases a relevant person may be satisfied the customer is who they say they are without needing to verify all suggested components of identity for example; residential address of the customer. This is acceptable provided sign off is obtained by senior management to ensure the relevant person is satisfied it is meeting its obligations under the Code.

[1] It is suitable for a risk based approach to be taken in respect of the identification information obtained in relation to parties connected to the relationship where the full components of identification information may not be available. For example, this may be the case for known beneficiaries where name, DOB and address might be the extent of information known. However, it must be ensured that if a payout is made the party is appropriately identified and their identity verified in line with the Code requirements.

7.1. Natural persons

In the case of natural persons, verification of identity comprises:

(1) Verification of identification information:

For all customers:
(i) name;
(ii) date of birth;

For standard and higher risk customers:
(iii) place of birth and / or nationality[2];
(iv) an official personal identification number; and

(2) Verification of permanent residential address[3] (including postcode if possible).

7.2. Legal persons

In the case of legal persons, verification of identity comprises:

1) Verification of identification information:
   (i) name;
   (ii) official identification number; and
   (iii) date and country of incorporation.

2) Verification of addresses:
   (i) registered office address/business address; and
   (ii) address of the principal place of business where this is different to the registered office/business address.

3) Verification of the identities of any natural persons associated with the legal person that are required to be identified as per the requirements of the Code.

7.3. Legal arrangements

In the case of legal arrangements, verification of identity comprises:

1) Verification of identification information:
   (i) name;
   (ii) date of establishment;
   (iii) official identification number; and

[2] A risk based approach should be taken and nationality and / or place of birth are verified wherever it is practical to do so.
[3] If a different address is used for correspondence with a customer the relevant person must be comfortable in relation the rationale of using that correspondence address, and the validity of the address, particularly if sending any personal documentation to that address.

(iv) legal status of the arrangement (i.e. satisfactory appointment of the trustee(s) nature of duties etc;

2) Verification of addresses:
   (i) the mailing address(es) of trustee(s) (or other person controlling the applicant); and

3) Verification of the identities of any natural persons associated with the legal arrangement that are required to be identified as per the requirements of the Code.

7.4. ID&V requirements for multiple signatories/directors

In relation to signatories, it is acknowledged that there may be a large number of signatories at different levels. Relevant persons should take a pragmatic view in identifying the signatories of a customer. The relevant person should take a risk based approach and form a view of which signatories are likely to be used to sign off certain activity or transactions and are deemed to be acting on behalf of the customer. Also, the level of signing powers should be considered and a view taken on whether the signatory's power is deemed to be significant. This information would usually be determined following a discussion with the customer.

In all cases it is expected that the relevant person should obtain a list of (but not necessarily obtain full identification information on or verify the identity of) all signatories and directors (or equivalent i.e. council members), for example by obtaining a copy of the register of directors (or equivalent). This information is important when conducting the customer's risk assessment in order to determine whether there could be any higher risk persons or PEPs associated with the customer.

It is expected that those persons with whom the relevant person has frequent interaction with or takes instructions from (be they directors or signatories) should be ID&Vd (subject to a minimum of 2 of the individuals).

In the case of a higher risk entity, it should be considered whether it is necessary to ID&V all of the directors and the signatories. However, it is noted that this may be impractical, for instance with a large multinational company, or a large international charity. If not all signatories and directors are ID&Vd the rationale behind not obtaining all of them should be documented.

In exceptional cases, where none of the fully ID&Vd third parties are available and in order not to disrupt essential business, another person may act as a signatory. This is provided the following conditions are met:

- the person is fully ID&Vd as soon as reasonably practicable after the event;
- the customer has not been identified as posing a higher risk of ML/FT;
- the risks of ML/FT are effectively managed;
- the relevant person has not identified any suspicious activity; and

- senior management approval is obtained for this activity until adequate verification of identity is received and the relevant person appropriately limits and monitors the transactions.

7.5. ID&V requirements for multiple 3rd parties

On occasion a customer may request a relevant person to allow a number of third parties to have limited control over their affairs such as a power of attorney. It is important that the relevant person understands and documents the rationale for such an arrangement and is comfortable with it from an AML/CFT point of view.

Where there could be a large number of potential third parties in this position, such as staff members at a certain company, the relevant person should obtain a list of the names and accompanying signatures of all potential third parties and fully ID&V those third parties that are expected to exercise control.

In exceptional cases, where none of the fully ID&Vd third parties are available and in order not to disrupt essential business, another person from the list may act as third party. This is provided the following conditions are met:

- the person is fully ID&V'd as soon as reasonably practicable after the event;
- the customer has not been identified as posing a higher risk of ML/FT;
- the risks of ML/FT are effectively managed;
- the relevant person has not identified any suspicious activity and
- senior management approval is obtained for this activity until adequate verification of identity is received and the relevant person appropriately limits and monitors the transactions.

7.6. ID&V requirements for clubs and associations

In the case of associations, clubs, societies, charities, church bodies, institutes, mutual and friendly societies, co-operative and provident societies, those with ultimate control will often include members of the governing body or committee plus executives. In the case of central and local government departments and agencies, this will include persons exercising control or significant influence over the department or agency.

When considering which natural persons need to be ID&V'd the entity concerned should be treated the same as a legal person or arrangement depending on its structure. Also, relevant persons must obtain an appropriately certified copy of the board resolution or power of attorney (or other authority) that provides the individuals representing the corporate customer with the right to act on the institution's behalf.

Where there are significant numbers of individuals that need to be ID&Vd, please see the additional guidance in section 7.4 or 7.5 of this document in relation to the approach that can be taken.

In exceptional cases, where none of the fully ID&V'd third parties are available and in order not to disrupt essential business, another person from the list may act for the entity. This is provided the following conditions are met:

- the person is fully ID&V'd as soon as reasonably practicable after the event;
- the customer has not been identified as posing a higher risk of ML/FT;
- the risks of ML/FT are effectively managed;
- the relevant person has not identified any suspicious activity; and
- senior management approval is obtained for this activity until adequate verification of identity is received and the relevant person appropriately limits and monitors the transactions.

8. Methods to verify natural persons

This section sets out the methods that can be used to verify the identity and address of natural persons. If one of the suggested methods cannot be used the relevant person is able to exercise discretion in relation to the documentation obtained as long as this is subject to a risk based approach and is appropriately recorded and signed off by senior management. There is further guidance in this section in relation to what to do in these circumstances.

Where hard copy documents are used for verification purposes these should be suitably certified for non-face-to-face customers. Where electronic documents are submitted appropriate measures should be taken (and recorded) to verify their authenticity.

8.1. Acceptable methods to verify identity

At least one from this section		
Method		**Conditions**
1	Passport	Current & valid Bearing photograph of the individual
2	National identity card[4]	
3	Provisional or full driving licence[5]	
4	Known employer ID card	Current & valid Bearing photograph of the individual Lower risk customers only[6]
5	Birth certificates	Infants & minors only A parent / guardian should be ID&Vd also
6	Proof of age card	If unable to provide items 1-4 Current & valid Bearing photograph of the individual
7	Use of independent data sources, including electronic sources	If this is the sole method of verification it is only permitted in lower or standard risk circumstances Should carry out additional check number 1 below
PLUS…on a risk based approach, consider the following additional checks…		
Additional check No.1	Require payment for the product or service to be drawn from an account in the customer's name at a regulated credit institution	
Additional check No.2	Use independent data sources, including electronic sources	

[4] Please note that a driving licence or national identity card does not always verify nationality or place of birth. Therefore care must be taken to ensure appropriate verification of nationality and / or place of birth takes place for the customer if required. A further document may need to be obtained from the customer to verify this information where it is deemed necessary as part of a risk based approach

[5] As above.

[6] Section 3.3.1 of the Handbook sets out detail regarding what would constitute "lower" risk.

When documentation cannot be provided…
On occasion, a customer may not be able to provide any of the documentation listed in methods 1-6 or the relevant person may not be able to undertake the additional checks in options 1 and 2. In such circumstances the relevant person should adopt a case by case approach in determining what methods they will accept to verify the customer's identity. The relevant person must be satisfied as to the validity and veracity of any documents accepted. The relevant person should clearly document why they have been unable to verify the customer's identity using the methods listed above, what alternative measures they have taken to verify their customer's identity and why they feel that this is sufficient to satisfy the requirements of the Code. Senior management approval should be obtained on a case by case basis.
Guidance on international drivers permits…
Relevant persons should exercise caution regarding International Drivers' Permits/International Drivers' Licenses. These can be obtained from unauthorised and unscrupulous operators on the internet who do not conduct any identification checks on the applicant for the Permit/Licence, and are marketed, for example, as a means of falsifying identity, avoiding driving fines and bans, and avoiding taking a driving test. International Drivers Permits can be genuine documents, but only when issued by competent national authorities to the holder of a valid domestic driving permit (i.e. national full driving licence) issued for use in the country of residence. The permit effectively converts a national licence into one for international use in other countries where the national licence is not recognised. An International Drivers' Permit is not a stand-alone document.

8.2. Acceptable methods to verify address

Table 1 below sets out the standard acceptable methods for verifying a natural person's address (this applies regardless of risk). Table 2 sets out alternative verification methods that may be considered. However this should only be used where the standard methods are not practical in respect of the customer in question rather than as default methods.

Please note that a non-residential address for a natural person, such as a PO Box, is not acceptable under any circumstances. A "care of" address is also generally unacceptable other than on a fully explained, clearly documented and time-limited basis (this should not exceed 12 months). Such situations should be closely monitored by the relevant person.

8.2.1. Change of address

As explained in section 3.4.2 of the Handbook, where identification information obtained previously has changed such as residential address the new information

should be sought in order to be in compliance with the Code. It should be considered whether this new information should be verified on a risk based approach. Consideration should also be given as to whether this change may impact on the risk assessment of the customer. Activity such as this will often be a trigger to review the relationship, in particular the customer's CDD information

In relation to a change of address a relevant person may, on a risk based approach, use one of the alternative verification methods in table 2 below to verify the new address.

Table 1: Standard address verification methods

At least one from this section		
Method		**Conditions**
1	A recent account statement from a regulated bank, building society or credit card company	No more than 6 months old If the statement or bill is in an e-format it must clearly show the address of the property (not just the customer's email address)
2	A recent mortgage statement from a regulated lender	
3	A recent rates, council tax or utility bill (not including a mobile telephone bill)	
4	Correspondence from an official independent source such as a central or local government department or agency in a List C jurisdiction	No more than 6 months old & Received by the customer in the post
5	Photographic driving licence or national identity card containing their current residential address	Current and valid Must not have been used as the sole document to verify identity
6	A documented record of a personal visit by a member of the relevant person's staff to the individual's residential address	n/a
7	Use independent data sources, including electronic sources.	n/a
PLUS…on a risk based approach, consider the following additional checks…		
Additional check No.1	Use independent data sources, including electronic sources.	
Additional check No.2	Make a physical validation by: • Making a telephone call to the customer with a telephone number that has been independently verified as belonging to the address in question; or • Sending a letter by registered post or courier to the address in question requiring the customer to respond with a signed confirmation of receipt or confirm to the relevant person a password or code contained in that letter.	
When documentation cannot be provided…		
On occasion, a customer may not be able to provide any of the documentation listed above or the relevant person may not be able to undertake the additional checks in options 1 and 2. There is therefore a further list below in table 2 of alternative methods that may also be used.		

Where the suggested validation checks are unable to be undertaken the relevant person should use a cumulative approach to ensure they are comfortable with the verification of the customer's address and the validity and veracity of the documents provided.

The relevant person should clearly document why they have been unable to verify the customer's address. It should be clearly documented what alternative measures have been taken to verify their customer's address and why they feel that this is sufficient to satisfy the requirements of the Code. Senior management approval should be obtained on a case by case basis.

Table 2: Alternative address verification methods

At least one from this section		
Method		**Conditions**
1	Lawyer's confirmation of a property purchase or legal document recognising title to the property.	Additional check No2 should be carried out where practical.
2	Tenancy agreement	
3	Checking a phone directory	if this is the sole method of address verification it should only be permitted in lower risk, face to face relationships Could be used as a cumulative method for all risk ratings
4	A letter from a known nursing home or residential home for the elderly confirming residence of the customer.	For UK and Isle of Man residents only
5	A letter from a director or manager of a known Isle of Man employer that confirms residence at a stated address, and indicates the expected duration of employment. In the case of a seasonal worker, the worker's residential address in his/her country of origin should also be obtained and, if possible, verified.	For Isle of Man residents and workers temporarily residing in the Isle of Man
6	A letter from a person of sufficient seniority at a known university or college that confirms residence at stated address. The student's residential address in the Isle of Man should also be obtained.	For students normally resident in the Isle of Man but studying off-Island.
7	A letter from a director or manager (including a person from the HR Department) of a verified known employer that confirms residence at a stated address (or provides detailed directions to locate a place of residence).	For overseas residents only. Detailed directions to be used where there is no

		formal address system in that area.
8	A letter of introduction confirming residential address from a trusted person (as defined in the Code) addressed to the relevant person. The trusted person must be able to confirm they have obtained and verified, or re-verified the individual's address information in the last 6 months.	Any customer unable to provide standard address verification in line with table 1.
9	Copy of contract of employment, or banker's or employer's written confirmation.	Additional check No2 should be carried out where practical.
PLUS…on a risk based approach consider at least one of the following…		
Additional check No.1	Use independent data sources, including electronic sources.	
Additional check No.2	Make a physical validation by: • Making a telephone call to the customer with a telephone number that has been independently verified as belonging to the address in question; or • Sending a letter by registered post or courier to the address in question requiring the customer to respond with a signed confirmation of receipt or confirm to the relevant person a password or code contained in that letter.	

9. Methods to verify legal persons

This section sets out the methods that can be used to verify the identity and address of legal persons. If one of the suggested methods cannot be used the relevant person is able to exercise discretion in relation to the documentation obtained as long as this is subject to a risk based approach and is appropriately recorded and signed off by senior management. Further guidance on what to do in these circumstances is provided in the table below.

Where hard copy documents are used for verification purposes these should be suitably certified for non-face-to-face customers. Where electronic documents are submitted appropriate measures should be taken (and these checks recorded) to verify their authenticity.

At least one from this section, ensuring that the identity, address and legal status are verified.			
Method		**What does this verify?**	**Conditions**
1	Certificate of Incorporation Memorandum (and / or Articles of Association) Equivalent document to the above (i.e. foundation charter)	ID	Must be either a certified copy or sourced directly from an independent public registry
2	Bank statement or utility bill	Address	No more than 6 months old. If the statement or bill is in an e-format it must clearly show the registered or correspondence address of the legal person (not just the customer's email address)
3	Latest Annual Return	ID and Address	Must be in date and sourced directly from an independent public registry
4	Audited financial statements which displays the company name, directors and registered address	All	Must be audited and signed by the auditor (photocopies or documents sourced from an independent public registry are acceptable)
5	Prepared accounts by a reporting accountant which displays the company name, directors and registered address	All	Must be signed by the reporting accountant
6	Conducting and recording an enquiry by a business information service, or an undertaking from a reputable and known firm of lawyers or accountants confirming the documents submitted	All	None

7	Undertaking a company registry search, including confirmation that the institution has not been, or is not in the process of being dissolved, struck off, wound up or terminated	Legal Status	Relevant person must be satisfied with legitimacy of the company registry being utilised
PLUS… on a risk based approach, consider the following additional checks…			
Additional check No.1	Require payment for the product or service to be drawn from an account in the customer's name at a regulated credit institution.		
Additional check No.2	Use independent data sources, including electronic sources		
When documentation cannot be provided			
On occasion, a customer may not be able to provide any of the documentation listed above or the relevant person may not be able to undertake the additional checks in options 1 and 2. In such circumstances the relevant person should adopt a case by case approach in determining what methods they will accept to verify the customer's identity. The relevant person must be satisfied as to the validity and veracity of any documents accepted. The relevant person should clearly document why they have been unable to verify the legal person's identity using the methods listed above, what alternative measures they have taken to verify the identity and why they feel that this is sufficient to satisfy the requirements of the Code. Senior management approval should be obtained on a case by case basis.			

10. Methods to verify legal arrangements

This section sets out the methods that can be used to verify the identity and address of legal arrangements. If one of the suggested methods cannot be used the relevant person is able to exercise discretion in relation to the documentation obtained as long as this is subject to a risk based approach and is appropriately recorded and signed off by senior management. Further guidance on what to do in these circumstances is provided in the table.

Where hard copy documents are used for verification purposes these should be suitably certified for non-face-to-face customers. Where electronic documents are submitted appropriate measures should be taken (and these checks recorded) to verify their authenticity.

At least one from this section, ensuring that the identity, address and legal status of the parties are verified as per sections 8 and 9 of this document as appropriate.			
Method		**What does this verify?**	**Conditions**
1	Trust Deed (or relevant extracts of the trust deed) and any subsequent deeds of appointment and retirement (or equivalent)	Evidences the formation of the arrangement and confirms that the persons in question are the trustees (or equivalent) of the arrangement	Must be a certified copy
2	Bank statement (if applicable)	Trustees Mailing Address	No more than 6 months old If the statement is in an e-format it must clearly show the mailing address (not just the customer's email address)
PLUS… on a risk based approach, consider the following additional checks…			
Additional check No.1	Require payment for the product or service to be drawn from an account in the customer's name at a regulated credit institution		
Additional check No.2	Use independent data sources, including electronic sources		
Additional check No.3.	Consider obtaining sight of the letter of wishes, or other relevant documents of the trust, to confirm the beneficiaries / potential beneficiaries to the trust.		
When documentation cannot be provided			
On occasion, a customer may not be able to provide any of the documentation listed above or the relevant person may not be able to undertake the additional checks in options 1 - 3. In such circumstances the relevant person should adopt a case by case approach in determining what methods they will accept to verify the customer's identity. The relevant person must be satisfied as to the validity and veracity of any documents accepted.			

The relevant person should clearly document why they have been unable to verify the person's identity using the methods listed above, what alternative measures they have taken to verify the identity and why they feel that this is sufficient to satisfy the requirements of the Code. Senior management approval should be obtained on a case by case basis.

11. Certification of hard copy documents

Use of an independent suitable certifier guards against the risk that hard copy documentation provided is not a genuine copy and in the case of identity documents that it corresponds to the customer whose identity is being verified. However, for certification to be effective, the certifier will need to have seen the original documentation and have met the individual face-to-face. Where a staff member of a relevant person meets the customer face-to-face they can certify the document, otherwise a suitable certifier must be used.

For non-face-to-face business suitable persons to certify documents include known and trusted members of the community such as:

- a member of the judiciary, a senior civil servant, a serving police or customs officer;
- an officer of an embassy, consulate or high commission of the country of issue of documentary verification of identity;
- a lawyer or notary public, who is a member of a recognised professional body;
- an accountant who is a member of a recognised professional body;
- a company secretary who is a member of a recognised professional body;
- a director, secretary or board member of a trusted person as defined in the Code; or
- a manager or other senior officer within the relevant person's group.

The certifier should sign and date the copy document (printing his/her name clearly in capitals underneath) and clearly indicate his/her position or capacity on it and provide contact details. The certifier should check the photograph represents a good likeness of the customer and should also state that it is a true copy of the original. There is no exact wording that has to be used, however the relevant person should ensure it covers the aforementioned areas.

The certifier may complete a covering letter or document, which is then attached to the copy identification document(s) i.e. the certification is not written on the copy identification document itself. This is suitable as long as the covering document contains the information specified in the paragraph above, and it is clear in the letter itself that it refers to the attached document.

In order to comply with the Code, relevant persons should satisfy themselves as to the suitability of a certifier based on the assessed risk of the business relationship and the reliance to be placed on the certified documents. In determining the certifier's suitability, a relevant person may consider factors such as the stature and track record of the certifier, previous experience of accepting certifications from certifiers in that profession or jurisdiction, the adequacy of the AML/CFT framework in place in the jurisdiction in which the certifier is located and the extent to which the AML/CFT framework applies to the certifier.

Relevant persons should ensure that any certified documents they have received are accurate and up-to-date[7]. In any circumstance where a relevant person is unsure of the authenticity of certified documents, or that the documents actually relate to the customer, a cumulative approach should be taken and additional measures or checks undertaken to gain comfort. If still unsatisfied with the verification of identity or address the business relationship must proceed no further, the relevant person must terminate the business relationship and consideration be given to making an internal disclosure.

Please see part 8.4 of the Handbook for details of the record keeping requirements in relation to these documents.

12. Use of electronic documents

Where a relevant person obtains verification documents electronically from the customer, original certification of these documents is not necessarily required. These documents should be provided to the relevant person as an image file or other tamper resistant format.

Below are some examples of electronic documentation that could be accepted, please note this is not an exhaustive list:

- In the case of an identity document (such as passport or driving licence) a photograph should be provided which clearly shows the person's face and the image on the identity document being held in the same picture to demonstrate this actually belongs to the customer. A clear scanned copy of the document itself should also be provided.

- A scanned copy of a certified document i.e. where a document has been certified in hard copy and is then scanned and emailed to the relevant person.

When considering the acceptability of electronic documents to verify a customer's identity, a relevant person should take a risk based approach to satisfy itself that the documents received adequately verify that the customer is who they say they are and that the relevant person is comfortable with the authenticity of these documents. The relevant person could check the type of file and ensure it is tamper resistant, it could check the email address it is being received from to ensure it seems legitimate and relates to the customer sending in the documentation, if the document has been certified that it is a suitable certifier etc.

In any circumstance where a relevant person is unsure of the authenticity of the documents, or that the documents actually relate to the customer, a cumulative approach should be taken and additional measures or checks undertaken to gain comfort. If still unsatisfied with the verification of identity or address the business relationship must proceed no further, the relevant person must terminate the business relationship and consideration be given to making an internal disclosure.

[9] Any document(s) provided must have been certified within 1 year and the document(s) must still be valid at the time it is being provided.

Please see part 8.4 of the Handbook for details of the record keeping requirements in relation to these documents.

13. Independent electronic data sources

Independent data sources can be used in certain circumstances to electronically verify a customer's identity and address. Note that independent electronic data sources may be used to verify that documents are authentic, but will not necessarily verify that your customer is who they say they are. Therefore where independent data sources are used a further verification method should be undertaken alongside this method as explained in the tables within this section.

Independent electronic data sources can provide a wide range of confirmatory material without involving a customer and are becoming increasingly accessible. However, an understanding of the depth, breadth and quality of the data accessed will be important. The sources that are often used by electronic systems include the passport issuing office, driving licence issuing authority, companies registry, the electoral roll and other commercial / electronic databases.

Where a relevant person intends to use electronic data sources conducted by commercial agencies, it should be sure that the agency is registered with a data protection agency in the European Economic Area. Relevant persons should also satisfy themselves that the agency:

- uses a range of positive information sources that can be called upon to link a customer to both current and historical data;
- accesses negative information sources such as databases relating to fraud and deceased persons;
- accesses a wide range of alert data sources; and
- has transparent processes that enable a relevant person to know what checks have been carried out, and what the results of these checks are.

Relevant persons should also ensure that:

- the source, scope and quality of the data are satisfactory. At least two matches of each component of an individual's identity or address should be obtained (careful thought should be given to searching with variations on spelling of the individual's name); and
- the processes allow the business to capture or store the information used to verify identity and/or address.

14. Purpose and intended nature of business relationship

The Code states at paragraphs 8 and 11 that information should be obtained in relation to the nature and intended purpose of each new business relationship or occasional transaction.

Unless it is obvious from the product being provided, the following information should be obtained to assist in meeting the Code requirements:

In all situations:

- expected type, volume and value of activity;
- expected geographical sphere of the activity; and
- details of any existing relationships with the product/service provider.

For legal persons and arrangements:

- an understanding of the ownership and control structure of the company, including group ownership where applicable as per paragraph 12 of the Code;
- nature of activities undertaken (having regard for sensitive activities and trading activities);
- geographical sphere of the legal person's activities and assets; and
- name of regulator (if any).

15. Source of funds and source of wealth

The Code requires at paragraphs 8 and 11 that a relevant person must take reasonable steps to establish the source of funds for all customers when entering a new relationship or carrying out an occasional transaction.

Paragraphs 14 and 15 of the Code also state that relevant persons must take reasonable steps to establish the source of wealth for higher risk customers (including higher risk domestic PEPs) and all foreign PEPs and also when unusual activity occurs.

At this time please see the standalone guidance document in relation to the source of funds and source of wealth information at this time until the main AML/CFT Handbook is updated (aiming for 2020).

16. Bearer shares

Many jurisdictions, including the Isle of Man, have prohibited or immobilised bearer shares due to the associated AML/CFT risks. However, certain jurisdictions may still allow these to be used therefore relevant persons must take particular care to record the details of bearer shares received or delivered other than through a recognised clearing or safe custody system, including the source and destination.

To reduce the opportunity for bearer shares to be used to obscure information on beneficial ownership, the Authority expects all relevant persons to immobilise bearer shares and take them into safe custody. Should a prospective, or existing, customer refuse to allow the immobilisation of the bearer shares, the relevant person should not proceed any further with the business relationship, and must consider making an internal disclosure.

17. Politically Exposed Persons ("PEPs")

17.1. PEP risk

Much international attention has been paid in recent years to the 'politically exposed person' ("PEP"), with the Financial Action Task Force ("FATF") having produced a guidance document relating to PEPs. PEP risk refers to the risks associated with providing financial and business services to those with a high political profile or who hold public office. The increased risk stems from the possibility of the PEP misusing their position and power for personal gain through bribery or corruption. Family members and close associates of PEPs may also pose a higher risk as PEPs may use family members and/or close associates to hide any misappropriated funds or assets gained through abuses of power, bribery or corruption. Investigations regarding proceeds of corruption often gain publicity and can damage the reputation of both the businesses and countries involved therefore it is important that a relevant person takes their responsibility to identify PEPs seriously.

Being a PEP does not mean that the individual should automatically be classified as higher risk of ML. This is because a large percentage of PEPs do not abuse their power nor are they in a position to abuse their power. However, relevant persons should be aware that an individual who has been entrusted with a prominent public function is likely to have a greater exposure to bribery and corruption.

The risks relating to PEPs increase when the person concerned has been entrusted with a political or public office role by a jurisdiction with known problems of bribery, corruption or financial irregularity within their government or society. The risk is even more acute where such countries do not have adequate AML/CFT standards, or where they do not meet financial transparency standards. Relevant persons should take appropriate measures to mitigate those risks.

17.2. PEP definitions

Domestic PEP – a PEP who is or has been entrusted with prominent public functions in the Island and any family members or close associates of the PEP, regardless of location of that PEP those family members or close associates.

Foreign PEP – a PEP who is or has been entrusted with prominent public functions outside the Island and any family members or close associates of the PEP regardless of the location of those family members or close associates.

Politically exposed persons are defined in paragraph 3 of the Code and include natural persons who are or have been entrusted with prominent public functions and their immediate family members and close associates. This definition would include royal families as persons entrusted with prominent public functions. The Code definition is:

"politically exposed person" or "PEP" means any of the following –

(a) A natural person who is or has been entrusted with prominent public functions ("P"), including -

(i) a head of state, head of government, minister or deputy or assistant minister;
(ii) a senior government official;
(iii) a member of parliament;
(iv) a senior politician;
(v) an important political party official;
(vi) a senior judicial official;
(vii) a member of a court of auditors or the board of a central bank;
(viii) an ambassador, charge d'affaires or other high-ranking officer in a diplomatic service;
(ix) a high-ranking officer in an armed force;
(x) a senior member of an administrative, management or supervisory body of a state-owned enterprise; or
(xi) a senior member of management of, or a member of, the governing body of an international entity or organisation.[8]

(b) any of the following family members of P, including –

(i) a spouse;
(ii) a partner considered by national law as equivalent to a spouse;
(iii) a child
(iv) a spouse or partner of a child;
(v) a brother or sister (including a half-brother or half-sister);
(vi) a spouse or partner of a brother or sister;
(vii) a parent;
(viii) a parent-in-law;
(ix) a grandparent; or
(x) a grandchild;

(c) any nature person known to be a close associate of PEP, including –

(i) a joint beneficial owner of a legal person or legal arrangement, or any other close business relationship, with P;

[8] The position of "honorary consul" has been removed from the PEP definition in the Code as part of the AML/CFT framework update. Whilst this has been removed relevant persons should remain aware of the potential risks associated with honorary consuls and may choose to continue to identify honorary consuls as PEPs although they are under no obligation to do so.

(ii) the sole beneficial owner of a legal person or legal arrangement known to have been set up for the benefit of P;
(iii) a beneficiary of a legal arrangement of which P is a beneficial owner or beneficiary; or
(iv) a person in a position to conduct substantial financial transactions on behalf of P.

An 'international entity or organisation', as defined at (a) (xi) above, refers to entities established by formal political agreements (international treaties) between their member states; their existence is recognised by law in their member countries and they are not treated as resident institutional units of the countries in which they are located. Examples of international organisations include, but are not limited to:

- the United Nations ("UN") and any affiliated international organisations;
- institutions of the European Union;
- the Council of Europe ("CoE");
- the North Atlantic Treaty Organisation ("NATO");
- the World Trade Organisation ("WTO");
- the International Monetary Fund ("IMF");
- the World Bank; and
- the Organisation for Security and Cooperation in Europe ("OSCE").

17.3. PEP requirements

Paragraph 14(1) of the Code states that a relevant person must:

establish, record, maintain and operate appropriate procedures and controls for the purpose of determining whether any of the following is, or subsequently becomes, a PEP —
(a) any customer;
(b) any natural person having power to direct the activities of a customer;
(c) any beneficial owner or known beneficiary; and
(d) in relation to a life assurance policy, the beneficiary and any beneficial owner of the beneficiary.

(2) A relevant person must establish, record, maintain and operate appropriate procedures and controls for requiring the approval of its senior management before —
(a) any business relationship is established with;

(b) any occasional transaction is carried out with; or

(c) a business relationship is continued with,
a domestic PEP who has been identified as posing a higher risk of ML/FT, or any foreign PEP.

(3) A relevant person must take reasonable measures to establish the source of wealth of -
(a) a domestic PEP who has been identified as posing a higher risk of ML/FT; and

(b) any foreign PEP.

(4) A relevant person must perform ongoing and effective enhanced monitoring of any business relationship with —
(a) a domestic PEP who has been identified as posing a higher risk of ML/FT; and

(b) any foreign PEP.

As stated at 14(4) above, the Code requires that enhanced monitoring is undertaken in relation to any business relationship with a foreign PEP and any higher risk domestic PEPs. The Authority would expect enhanced monitoring of these particular categories of PEPs to take place at least annually.

Where the requirements of paragraph 14 of the Code are not met within a reasonable timeframe, as per 14(6) of the Code, the procedures and controls must provide that:

(a) the business relationship or occasional transaction must proceed no further;

(b) the relevant person must consider terminating the relationship; and

(c) the relevant person must consider making an internal disclosure.

The requirements in paragraph 14 of the Code must also be met in addition to any EDD requirements under paragraph 15 where the customer may also have been identified as posing a higher risk. It is important to appreciate that although it is likely that a PEP will pose a higher risk, this is only one of a number of factors that should be considered when determining the risk rating of the customer. For example, if a PEP operates a bank account which has a small turnover from expected salary, payments in and debits out to cover household and living expenses, in an equivalent jurisdiction, then this may reasonably be assessed as not posing a higher risk of ML/FT.

Where a PEP has not been identified as posing a higher risk of ML/FT they can treated like any other customer and the normal Code requirements apply.

The requirements of paragraphs 14(2), (3) and (4) of the Code apply to all foreign PEPs or any domestic PEPs that have been assessed as posing a higher risk. It is important to

recognise that the definitions of domestic PEP and foreign PEP are based on where the PEP's prominent function relates to rather than the residency of the individual.

When a PEP has been identified as higher risk and the relevant person has a detailed knowledge of the PEP, it is important that the relevant person does not assume that the detailed knowledge allows for the PEP to be treated as anything other than higher risk. The additional PEP requirements EDD measures set out in the Code should always be applied where relevant, regardless of a detailed knowledge of the PEP.

For the avoidance of doubt, where a PEP is not considered higher risk, the reasons for this should be documented, and the individual must still be identified as a PEP.

The below table summarises the requirements in relation to PEPs:

Customer	EDD (Para 15)	Additional PEP req's (Para 14 (2-5))
High risk domestic PEP	Yes	Yes
Standard risk domestic PEP	No	No
High risk foreign PEP	Yes	Yes
Standard risk foreign PEP	No	Yes

17.4. Identifying PEPs

Paragraph (14)(1) of the Code requires a relevant person to establish, record, maintain and operate appropriate procedures and controls for the purpose of determining whether any of the following is, or has subsequently become, a PEP –

> (a) any customer;
> (b) any natural person having power to direct the activities of a customer;
> (c) any beneficial owner or known beneficiaries; and
> (d) in relation to a life assurance policy, the beneficiary and any beneficial owner of the beneficiary.

When identifying if a customer is a PEP, a relevant person can utilise various methods of identification, including commercially available databases and screening tools. It can also be useful to research who the current and former holders of prominent public functions are, both locally and internationally. Various sources could be consulted to determine who holds or formerly held the prominent public functions, such as Tynwald, the UK Government, the European Parliament and international organisations including the UN and World Bank. In addition, the equivalent jurisdiction List in Appendix C and the high risk jurisdiction Lists and jurisdictions that may pose a high risk in Appendix D(a) and D(b), respectively, can be consulted.

Whilst the definition of PEP focuses on positions of prominent public function, it is important for relevant persons to be aware of the risk of junior officials being used by PEPs to bypass AML/CFT controls. Consideration can be given to assessing the extent to which an individual could be used by a PEP and the associated risks.

The obligation to identify PEPs does not end once the customer relationship has been formed. Paragraph 13 of the Code requires a relevant person to perform ongoing and effective monitoring of any business relationship. Relevant persons should ensure that the procedures for identifying PEPs and ongoing monitoring are clear regarding identifying if any individuals have *become* PEPs since the business relationship was formed.

There is also a common misconception is that PEPs who have immunity from prosecution or conviction, such as Heads of State immunity in office for actions committed prior to taking office or diplomats, are not subject to PEP requirements. It is important to understand that this is not the case; having knowledge of a PEP with immunity could lead to discovering information used in a SAR which in turn could trigger an investigation into individuals who do not have immunity.

17.5. Identifying PEP risk

Identifying that a client is a PEP forms part of the wider process of establishing the risks relating to your customers. Whilst individuals who are PEPs should not be prejudged as having links to criminal activity or abuse of the financial system, a relevant person should be aware of the risks associated with PEPs.

The FATF has developed a list of indicators and red flags which can assist in the detection of any potential misuse of the financial system by PEPs. These red flags have not been developed to stigmatise all PEPs, rather they are an aid to detect PEPs who are abusing the financial system. Matching one or more red flags may only raise the risk of doing business with the relevant PEP however in certain circumstances, matching one or more red flags could lead to a direct money laundering or terrorist financing suspicion.

The list of indicators/red flags developed by the FATF is not an exhaustive list and should be used in conjunction with the other factors to determine the risks of customers. Please refer to Annex 1 of the FATF guidance paper on politically exposed persons for red flags relating to areas such as:

- PEPs shielding their identity;
- A PEP's position in a business;
- The industry/sector the PEP is involved in; and
- Country specific indicators.

Other examples of indicators of corruption include excessive revenue from consultancy fees or commissions, where there are inexplicable commissions being paid out or where there may be contracts with escalated prices.

Indicators can also be helpful in determining whether a PEP is lower risk. Lower risk indicators can include areas such as:

- The relevant prominent public function being conducted in a country associated with low levels of corruption;
- The relevant prominent public function being conducted in a country with a track record of investigating political corruption;
- The PEP being subject to rigorous disclosure requirements; and
- The PEP does not have executive decision-making responsibilities.

The above is not an exhaustive list. Any decision to rate a PEP as lower risk should have a clear rationale and be clearly documented.

17.6. "Once a PEP, always a PEP"?

Paragraph 3 of the Code states that a PEP is a natural person who is or has been entrusted with a prominent public function, their family members and close associates.

The Authority expects a relevant person to assume the default position of 'once a PEP, could always remain a PEP' when a PEP is no longer in that prominent public function. This is in line with the guidance issued by the FATF in 2013, which states that the treatment of PEPs should be based on an assessment of risk rather than prescribed time limits. When a PEP is no longer in the prominent public function, FIs and DNFBPs can utilise a risk based approach to determine the risks associated with the PEP.

An assessment of the risks associated with the jurisdiction, the seniority of the role as well as the individual PEP can be conducted in order to determine whether the PEP continues to represent a higher risk. Considerations can include:

- The nature and duration of the individual's role;
- How much time has passed since they were in the role;
- The level of (informal) influence that the individual could still exercise;
- Whether the individual's previous and current function are linked in any way (e.g. formally by appointment of the PEPs successor, or informally by the fact that the PEP continues to deal with the same substantive matters);
- The level of inherent corruption risk in the jurisdiction of their political exposure;
- The level of transparency about the source of wealth and origin of funds; and
- Links to higher risk industries.

This risk based approach can also be used where a PEP is deceased but this individual was the source of funds/source of wealth for family members and close associates who have been identified as high risk domestic or foreign PEPs. In such circumstances, an individual assessment should be conducted to determine whether the relationship still merits EDD measures.

If a relevant person chooses to utilise a risk based approach, they should ensure that a clear and detailed rationale, explaining why the individual should not be treated as a PEP, is documented. Any decision to use this approach should be subject to an appropriate level of senior management review and approval and where PEPs are no longer classified as such, their former PEP status should be documented.

Whilst a risk based approach can be utilised once a PEP is no longer in the prominent public function, it is important for a relevant person to understand that a PEPs influence and prominence may not have diminished; PEPs in prominent roles may continue to have influence and power after they have left the role and thus be potentially more susceptible to bribery and corruption. In addition, a PEP may have been in a position to acquire their wealth illicitly when in the relevant role or function, therefore high level scrutiny may be warranted once they are no longer a PEP. A relevant person should be aware that the risks associated with PEPs are closely linked to the inherent corruption risk of the jurisdiction in which they held the role, the relevant role or function and the influence held during their post.