ISLE OF MAN
FINANCIAL SERVICES AUTHORITY

*Lught-Reill Shirveishyn Argidoil Ellan Vannin*

# Collective Investment Schemes ("Funds") & Businesses providing services to Collective Investment Schemes ("Functionaries")

## Sector Specific AML/CFT Guidance Notes

## July 2023



Contact:
AML/CFT 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 02
(First issued August 2021)

# Contents

# Version history

| | |
|---|---|
| Version 2 (July 2023) | 4.4 – removal of reference to paragraph 16<br><br>Updates made to links |

# 1. Foreword

This guidance is applicable to:

- Collective Investment Schemes within the meaning of section 1 of the Collective Investment Schemes Act 2008 ("CISA08") (which includes Exempt schemes) ("funds" or "schemes"); and
- businesses providing services to Collective Investment Schemes, licensed to carry on regulated activities falling within Class 3 of the Regulated Activities Order 2011, whether or not an exemption specified in the Financial Services (Exemptions) Regulations 2011 ("Exemptions Regulations") applies to that activity (known as the "functionaries").

Paragraph 2(6)(b) of schedule 4 to the Proceeds of Crime Act 2008 states that the Anti-Money Laundering and Countering the Financing of Terrorism Code 2019 ("the Code") applies to:

> a collective investment scheme within the meaning of section 1 of the *Collective Investment Schemes Act 2008*

Paragraph 2(6)(a) of schedule 4 to the Proceeds of Crime Act 2008 states that the Code applies to:

> subject to sub-paragraph (13), engaging in any regulated activity within the meaning of the *Financial Services Act 2008*, whether or not an exemption specified in the Financial Services (Exemptions) Regulations 2011, as those Regulations have effect from time to time and any instrument or enactment from time to time amending or replacing those Regulations, applies to that activity;

***The requirements of the Code therefore apply to all funds established in the Isle of Man, and to all Isle of Man functionaries.***

The Code also applies to exempt managers, asset managers and investment advisers to specialist funds (paragraph 3.9 of the Exemptions Regulations), managers of Exempt and exempt-type schemes when providing services to no more than one scheme (paragraph 3.2 of the Exemptions Regulations) and Exempt managers of Experienced Investment Funds (paragraph 3.3 of the Exemptions Regulations).

Both funds and functionaries are relevant persons for the purposes of the Code.

# 2. Introduction

The purpose of this document is to provide guidance specifically for funds established under CIS08, and functionaries, in relation to Anti-Money Lundering and Countering the Financing of Terrorism ("AML/CFT"). This document should be read in conjunction both with the Code and the main body of the AML/CFT Handbook ("the Handbook").

Though the guidance in the Handbook, and this sector specific guidance, is neither legislation nor constitutes legal advice, it is persuasive in respect of contraventions of AML/CFT legislation dealt with criminally, by way of civil penalty or in respect of the Authority's considerations of a relevant person's (as such a term is defined in paragraph 3 of the Code) regulatory / registered status and the fit and proper status of its owners and key staff where appropriate.

## 2.1 Relationship between a fund and its functionary

In practice an Isle of Man fund will delegate the majority (if not all) of AML/CFT activities to its functionaries (fund manager/administrator); however, the fund must understand and document what services the functionary is, and more importantly is not, providing in relation to the fund's obligations under the Code. This should be considered at the outset of the relationship and included as part of the functionary agreement between the fund and the Manager or Administrator. The services/agreement document should also be reviewed on a regular basis.

Functionaries' customers are the funds themselves. Functionaries are responsible for assessing the money laundering and financing of terrorism ("ML/FT") risk associated with the take on of funds as customers and the ongoing risks of the customer relationship. This includes an understanding of not only the fund's investor base but also what the fund is investing in, the fund structure, and the other functionaries providing services to the fund.

This document covers ML/FT risks that may be faced by funds and functionaries and provides further guidance and clarification in respect of approaches to customer due diligence, and other specific matters relevant to the sector.

This document also takes into account, where applicable, the following documents:

- FATF guidance for a risk-based approach - Securities Sector (2018);
- FATF report – Money Laundering and Terrorist Financing in the Securities Sector (2009);
- MONEYVAL typology research – Use of securities in money laundering schemes (2008); and
- Joint Guidelines of ESA - Risk factor guidance (2017).

The Authority recommends that relevant persons familiarise themselves with these documents and other typology reports concerning funds and functionaries.

## 2.2 National Risk Assessment

The Island's National Risk Assessment ("NRA") was published in 2015 and was updated in 2020. Funds and functionaries must ensure their business risk assessments (and customer risk assessments where necessary) take into account any relevant findings of the NRA.

In relation to the main vulnerabilities of funds and functionaries, there can be some fairly complex structures and characteristics, particularly in non-retail funds. Also, there are often

a number of different parties involved in operating the business relationships (which are mostly non-face to face), therefore there could be gaps in compliance (by the fund) with the Code if the role of the functionaries is not fully understood, or documented, by the governing body of the fund. Robust documentation in this respect is important, as is the experience of the directors of the fund and the functionaries of the fund. The NRA sets out the main risks and vulnerabilities in detail.

Overall, after applying consideration of the control and other preventative measures in place, the sector is assessed as having a medium level of vulnerability for ML and a medium level of vulnerability for FT.

# 3. Responsibilities

## 3.1 General

| | Schedule 4 to POCA | The Code | Who is the customer? | Responsibilities | Agreements |
|---|---|---|---|---|---|
| Fund | 2(6)(b) | The fund must comply with all provisions of the Code.<br><br>Activities and reporting under the Code, such as CDD and ongoing monitoring, may be delegated to functionaries.<br><br>Further guidance is provided in section 3 below. | The investors into the fund. | As per paragraph 4(3) of the Code, the ultimate responsibility for ensuring the fund's compliance with the Code is that of the fund (the governing body). | Rule 6.60 (Requirement for written functionary agreement) of the Financial Services Rule Book 2016 requires that an agreement will be in place between a fund and its functionary which sets out the services that are to be provided.<br><br>These agreements should clearly set out the roles and responsibilities of each entity with regards to the fund's compliance with the Code, e.g. the ownership of records in relation to CDD and customer risk assessments at fund level.<br><br>Agreements should also clearly document how the fund will monitor and oversee the work of its delegate with regards to the fund's compliance with the Code (including clearly stating if the functionary is providing the fund's MLRO. The MLRO does not need to be named in the agreement, but the fund should be aware of who is the MLRO).<br><br>It is important that a fund is able to demonstrate how it has complied and remains compliant with all areas of the Code, to do this will require reporting from those undertaking activities on its behalf.<br><br>Where existing agreements do not clearly set out the roles and responsibilities of each entity this could be dealt with by way of a side letter or addendum. |
| Functionary | 2(6)(a) | The functionary must comply with all provisions of the Code in relation to its own activities and also in relation to the fund if a delegation is in place with regards to the fund's compliance with the Code. | The fund to which they are providing services i.e. the directors / owners of the management shares of the fund. | The functionary must comply with the Code in its own right. | |

## 3.2 The role of the MLRO

Both the fund and functionary, as relevant persons for the purposes of the Code, must appoint a Money Laundering Reporting Officer ("MLRO") to exercise the reporting functions under paragraphs 25 and 27 of the Code. They must both establish, record, maintain and operate appropriate reporting procedures and controls to enable internal and external disclosures to be made.

The fund itself can meet its obligations in relation to the reporting procedures of the MLRO by:

- implementing the procedures and controls directly; or
- if the fund has no executive staff and the administration of its investors is undertaken by an IOM functionary, the fund will be considered compliant with the Code if it has formally delegated the activity to the functionary by way of agreement or other evidence of mutual agreement of the arrangements by both parties.

### 3.2.1 External disclosures

For the avoidance of doubt, both the fund and the functionary are required to make an external disclosure where a functionary is providing services to a fund and the functionary detects suspicious activity in relation to the fund's customers. In practice, the functionary may be providing all services to the fund, including the MLRO; in these cases it is acceptable for one external report to be submitted on behalf of both the fund and the functionary. Where this is done the external disclosure should clearly state in the grounds section that it is being made on behalf of both the fund and the functionary.

Reporting of external disclosures is undertaken through the Themis system; Themis is also used by the FIU for disseminating information and serving notices. Therefore, all relevant persons should be registered on Themis.

## 3.3 Services to overseas schemes

Overseas and recognised schemes are subject to the AML/CFT regimes of the jurisdictions that they are established in. Isle of Man functionaries who are carrying out AML/CFT activities for such schemes need to be aware of the AML/CFT obligations of the fund that they are acting for. When conducting a Customer Risk Assessment ("CRA") on an overseas fund a functionary should consider the AML/CFT regime of that particular jurisdiction, as part of its consideration of the location of the customer's activities required by paragraph 6(3)(b) of the Code.

If a staff member of a functionary is appointed as the MLRO of an overseas or recognised fund they should ensure that they are fully aware of the legislative and reporting requirements that the fund is subject to.

Regardless of where the fund is located the Isle of Man functionary must comply with the Code in respect of their customer (fund).

### 3.4 Services to another functionary

Where a functionary is providing Class 3(9) or (10) services to another functionary, that functionary is their customer.

Where a functionary ("functionary A") is providing services to the manager or administrator ("functionary B") of a fund, and functionary B is located outside the island, functionary A needs to be aware of the legislative requirements that functionary B is subject to and ensure that it is considered as part of the customer risk assessment that it undertakes for functionary B.

In such instances, functionaries may wish to consider utilising the simplified measures permitted under paragraph 16 of the Code, for the purpose of verifying the identity of the other functionary. It should be noted that, whilst group entities may be able to use the exemptions and simplified measures detailed in Part 6 of the Code if the relevant conditions are met, there are no additional concessions available in relation to group entities.

As per Rule 6.60 (Requirement for written functionary agreement) of the Financial Services Rule Book, an agreement must be in place between the two functionaries setting out the services that are to be provided, under Class 3(10).

As per rule 8.12 (Contractual arrangements for management and administration) of the Financial Services Rule Book, written contractual arrangements must be in place between the Class 3(9) licenceholder and the person to which it provides management or administration services.

## 4. Who is the fund's customer?

The complexity of the funds sector and the variety of intermediary roles that may be involved in a business relationship highlights how difficult it is to document examples that will fit all scenarios. Therefore it is important for relevant persons in this sector to understand the business relationship and apply a risk based approach to mitigate any ML/FT risks identified. The main different types of business relationship (between a fund and its customers) are described below (sections 4.1 to 4.4 of this document).

For all fund customers, the relevant person (the fund, or the functionary to whom the fund has delegated certain matters to) must have documented steps that are utilised and evidenced to determine whether a customer is acting on behalf of another person (as per paragraph 12(2)(b) of the Code). Section 3.4.5 of the Handbook gives guidance regarding identifying whether a customer is acting on behalf of another person.

## 4.1 Direct investor (not through an intermediary)

For instance: A natural or legal person, or a legal arrangement, ("investor"), that directly invests into the fund and directly buys units of, or shares in, a fund in their own name and not on behalf of any other party.

The fund's customer is the investor and the fund, or its functionary, must apply CDD measures (including ECDD and any required enhanced PEP measures) to that investor, including the beneficial owner of that investor in accordance with Part 4 (Customer due diligence and ongoing monitoring) of the Code. Depending on the nature of the investor, exemptions and simplified measures may be applicable under paragraphs 16 (Acceptable applicants), 19 (Eligible introducers) or 21 (Miscellaneous) of the Code , as long as all requirements are met, the investor has not been assessed as posing a higher risk and suspicious activity has not been identified.

## 4.2 Direct investor (through an intermediary)

For instance: A natural or legal person, or a legal arrangement, ("investor"), that invests into the fund and buys units of, or shares in, a fund in their own name using an intermediary. The intermediary is not the legal or registered owner of the shares or units and does not control or make decisions about the investment.

The fund's customer is the investor and the fund, or its functionary, must apply CDD measures (including ECDD and any required enhanced PEP measures) to that investor, including the beneficial owner of that investor in accordance with Part 4 (Customer due diligence and ongoing monitoring) of the Code. Depending on the nature of the investor, exemptions and simplified measures may be applicable under paragraphs 16 (Acceptable applicants), 19 (Eligible introducers) or 21 (Miscellaneous) of the Code, as long as all requirements are met, the investor has not been assessed as posing a higher risk and suspicious activity has not been identified.

## 4.3 Intermediary – it has been determined that the intermediary is not acting on behalf of another person

For instance: A financial institution (intermediary) that as part of its business activity, directly purchases the units of, or shares in, a fund in its own name and exercises control over the investment (which may be for the benefit of one or more third parties who do not control the investment or investment decisions), and where funds or income are returned to the registered owner (an account in the name of the intermediary).

In the above case the fund's customer is the intermediary and the fund, or its functionary, must apply CDD measures (including ECDD and any required enhanced PEP measures) to the intermediary. Exemptions and simplified measures may be applicable under paragraphs 16 (Acceptable applicants), 19 (Eligible Introducers) or 21 (Miscellaneous) of the Code, as long as all requirements are met, the customer (the intermediary) has not been assessed as posing a higher risk and suspicious activity has not been identified.

### 4.4 Intermediary – it has been determined that the intermediary is acting on behalf of another person ("third party")

For instance: A financial institution (intermediary) that acts in its own name and is the registered owner of the shares or units, but it is acting on the account of, and pursuant to specific instructions from one or more third parties.

The fund's customer is the intermediary and the fund, or its functionary, must apply CDD measures (including EDD and enhanced measures if required) to that intermediary. Exemptions and simplified measures may be applicable under paragraphs 19 (Eligible introducers) or 21 (Miscellaneous) of the Code, as long as all requirements are met, the customer (the intermediary) has not been assessed as posing a higher risk and suspicious activity has not been identified.

In addition, as the intermediary is acting on behalf of one or more third parties, the fund (or its functionary) must identify those third parties and take reasonable measures to verify their identity (as per paragraph 12(2)(b) of the Code). Section 3.4.5 of the Handbook gives guidance regarding identifying whether a customer is acting on behalf of another person. However, the functionary, undertaking the work for the fund, may be able to use the exemption for "Persons in a regulated sector acting on behalf of a third party" (paragraph 17 of the Code), as long as all requirements are met, including that the customer (the intermediary) has not been assessed as posing a higher risk and suspicious activity has not been identified.

## 5. Risk Guidance

Funds and their functionaries are part of a broad sector and the ML/FT risks will vary for each of them based on a wide range of factors such as the type of products and services they supply, their customers and delivery channels.

This document covers some of the general risk factors common to the sector and focuses on particular individual business types where necessary, but is not exhaustive. Each individual relevant person needs to consider its own risk profile.

As noted above both the funds themselves and functionaries are relevant persons for the purposes of the Code; each must prepare an assessment of its exposure to ML/FT risk - this includes a Business Risk Assessment ("BRA") (paragraph 5 of the Code), and an assessment of the risk of ML/FT that a business relationship or one-off transaction poses for each of its customers (the CRA paragraph 6 of the Code).

A Technology Risk Assessment ("TRA") (paragraph 7 of the Code) must also be carried out by each relevant person. If it is considered that there is no technology risk (either for the fund or the functionary) the considerations and conclusion should still be documented. The fund's TRA may be similar, and could be based upon, the TRA of its functionary. However, the fund must have its own distinct TRA, and clear consideration of the fund's own technological risks must take place.

It is common that a fund will delegate the conducting of its BRA, TRA and its CRAs to a functionary. If this is the case this should be clearly documented in the agreement required by Rule 6.60 (Requirement for a written functionary agreement) of the Financial Services Rule Book.

The fund's BRA may be similar to, and could be based upon, the CRA that the functionary prepares in respect of the fund as its customer. However, the fund must have its own separately documented BRA which meets all the requirements of paragraph 5 of the Code.

Vigilance should govern all aspects of the relevant person's dealings with its customers, including:

- account opening;
- customer instructions;
- transactions during the relationship;
- ongoing monitoring of the business relationship (including transactions);
- technology / security issues if there is an online element to the business relationship; and
- any outsourced / delegated services.

## 5.1 General Higher Risk Indicators

As with the basic elements of a risk assessment, discussed in chapter 2 of the Handbook, the following activities may increase the risk of the relationship. Just because an activity / scenario is listed below it does not automatically make the relationship higher risk, the customer's rationale / nature / purpose of the business relationship etc. should be considered in all cases.

If a relevant person is unable to obtain a satisfactory explanation from a customer in the event of the following situations, features, or activities, or any other features which cause it concerns, it should be determined whether this is suspicious or unusual activity. Please refer to chapter 5 of the Handbook for further detail of the Island's suspicious activity reporting regime.

As stated in paragraph 13 of the Code:

**13 Ongoing monitoring**

(2) Where a relevant person identifies any unusual activity in the course of a business relationship or occasional transaction the relevant person must –

(a) perform appropriate scrutiny of the activity;
(b) conduct EDD in accordance with paragraph 15; and
(c) consider whether to make an internal disclosure.

(3) Where a relevant person identifies any suspicious activity in the course of a business relationship or occasional transaction the relevant person must –

(a) conduct EDD in accordance with paragraph 15 of the Code, unless the relevant person believes conducting EDD will tip off the customer; and
(b) make an internal disclosure.

This list of higher risk indicators is by no means exhaustive, and relevant persons should be vigilant for any transactions where suspicion may be aroused and take appropriate measures. Please also see the list of red flags included at 5.2 of this document.

- Where a customer is reluctant to provide normal information or provides only minimal information.
- Where a customer's documentation cannot be readily verified.
- The customer is reluctant to provide the relevant person with complete information about the nature and purpose of the relationship including anticipated account activity.
- The customer is located in a higher risk jurisdiction.
- Transactions involving numerous jurisdictions.
- The customer has no discernible reason for using the relevant person's services, or the businesses' location.
- The customer's address is associated with multiple accounts that do not appear to be related.
- The nature of activity does not seem in line with the customer's usual pattern of activity.
- The customer enquiries about how to close accounts without explaining their reasons fully.
- The customer opens an account / product without any regards to loss, commissions or other costs associated with that account / product.
- The customer acts through intermediaries such as money managers or advisers in order not to have their identity registered.
- The customer exhibits unusual concern with the relevant person's compliance with Government reporting requirements / AML/CFT policies and procedures.
- Wire transfers / payments are sent to, or originate from higher risk jurisdictions without apparent business reason.
- The customer's transaction pattern suddenly changes in a manner that is inconsistent with the customer's normal activities or inconsistent with the customer's profile.

## 5.2 Red Flags

In addition to the above higher risk indicators, there are some factors that are likely to be "red flags" in relation to that particular relationship and would therefore usually be suspicious activity. If a relevant person identifies suspicious activity appropriate steps as explained in section 5 of this document, and the Code, must be taken. This list of red flags is by no means exhaustive and is as follows:

- where it is identified a customer provides false or misleading information;
- where it is identified a customer provides suspicious identification documents;
- the customer does not provide the relevant person with relevant / accurate information about the nature and intended or ongoing purpose of the relationship, including anticipated account activity;
- the customer is secretive / evasive when asked to provide more information;
- when requested, the customer refuses to identify a legitimate source of funds or source of wealth;

- the customer refuses to provide details on beneficial owners of an account or provides information which is false, misleading or substantially incorrect;
- the customer enquires how quickly they can end a business relationship where it is not expected;
- where the business relationship is ended unexpectedly by the customer and the customer accepts unusually high fees to terminate the relationship without question;
- the customer is known to have criminal / civil / regulatory proceedings against them for crime, corruption, misuse of public funds or is known to associate with such persons; and
- the customer is interested in paying higher charges to keep their identity secret.

## 5.3 Risk Factors specific to the sector

The following section of the guidance covers some of the risk factors specifically related to the funds industry. When considering these activities there could be both retail and non-retail customers. Further guidance surrounding risk assessments can be found in Part 3 of the Handbook.

Specific risk factors to consider (in addition to those noted in 5.1 and 5.2) may include:

### 5.3.1 Fund

- Unusual asset types.
- Complex structures.
- Rationale (does it make sense? are there any unusual features?).
- In specie transfers of assets.
- Related party transfer of assets and related party transactions.
- Payment methods – e.g. the use of crypto currency within the fund structure.
- The wide range of jurisdictions which may be involved.
- Exempt schemes - due to being more lightly regulated, these may be more susceptible to financial crime.

### 5.3.2 Investors

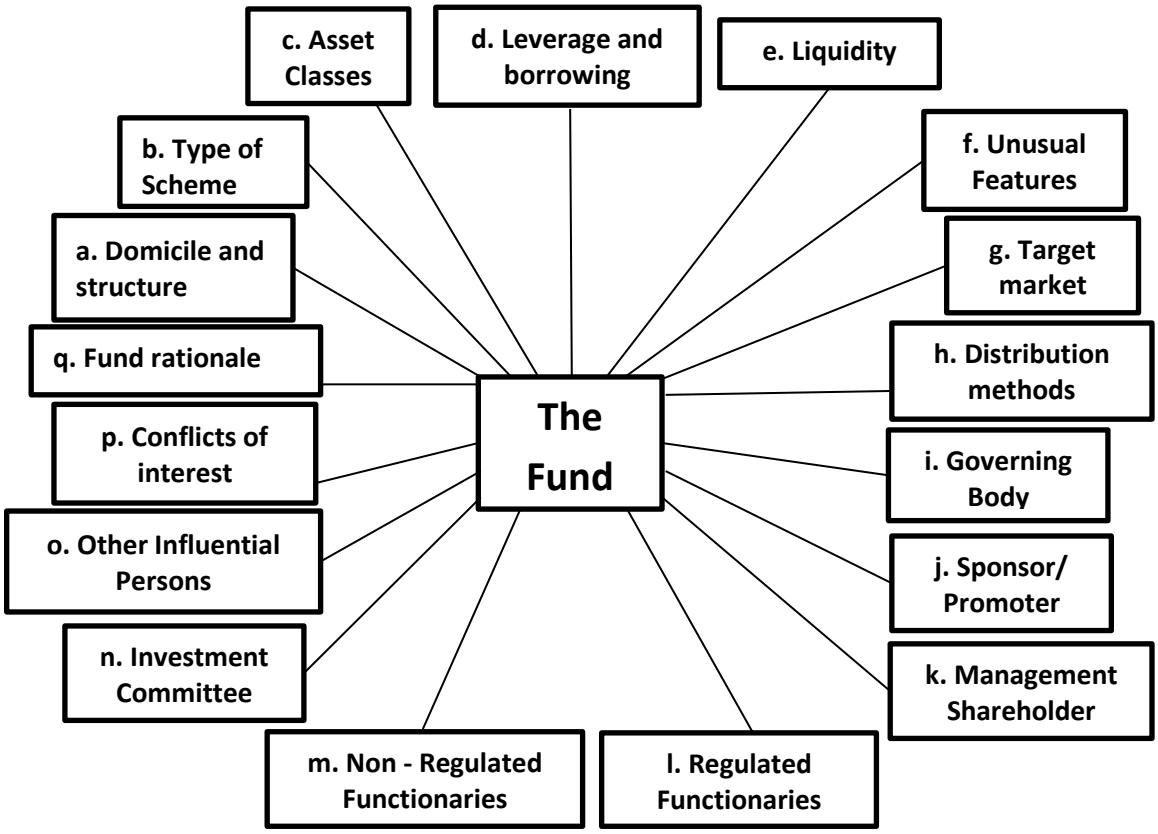
- Most transactions are conducted on a non-face-to-face basis. However, that risk could be mitigated by the fact that these transactions may involve a regulated introducer or nominee of that introducer (when relying on elements of due diligence provided by an introducer relevant persons must comply with Paragraph 9 of the Code).
- The tenure of the investment - most investment is made for medium and long-term objectives, transactions suggesting that improper use is being made of an investment fund will tend to centre on transactions held for a short time or multiple investments.
- The amount of the investment and whether this appears commensurate with the investor's circumstances.
- Holdings of investment funds may be transferred between different parties. Such transfers will be recorded by the registrar of the fund. Where transfers take place the new holder must be risk assessed and CDD must be conducted.
- The investor is undertaking many different transactions without a legitimate reason.
- The potential for payments to and from third parties.

- If the investor is another fund, high risk indicators may include:
  - aiming to invest in products that are susceptible to money laundering;
  - offering high rates of return;
  - has one off minimum investment amounts so that it operates below AML reporting thresholds;
  - highly liquid open ended frequent subscriptions and redemptions;
  - jurisdiction of the assets and advisors to the assets;
  - unregulated advisors;
  - adverse media; and
  - complex opaque structure.

### 5.3.3 Considerations when risk assessing a fund

In order for a functionary to have a full understanding of a fund, when completing the CRA of the fund under paragraph 6 of the Code they need to (in addition to other considerations) have an understanding of the fund's investor base, what the fund is investing in and the fund structure. The other functionaries and any related parties (for example those that contract with, or may have a relationship with, the fund, and may benefit, for example by receiving fees etc.) need to be identified and consideration given to whether any further information or due diligence is required. Diagram 1, and the table below, provide further information on matters to be considered during the CRA.

**Diagram 1 - Due Diligence considerations when undertaking a customer risk assessment of the fund should include:**



| Risk factors to consider when conducting a Fund CRA or BRA include, but are not limited to: | |
|---|---|
| a. Domicile and Structure | - Fund's jurisdiction<br>- Mind and management of the structure<br>- Lack of transparency in the structure<br>- Complexity in the structure of the fund (and the structure it is part of)<br>- Legal structure<br>- Separate Governing body/General Partner |
| b. Type of Fund | - Authorised/ Approved by a regulator<br>- Registered with a regulator<br>- Not subject to approval or registration (e.g. wholly or mostly unregulated)<br>- No or very limited regulatory oversight<br>- Open/closed |
| c. Asset Classes | - Listed assets<br>- Unlisted assets – is a valid valuation methodology in place?<br>- Unusual assets<br>- In specie transfer of assets, related party transfers.<br>- Use of SPV's<br>- Real estate (potential to manipulate valuations/security/rents). Do the properties as described exist?<br>- Valuers - experience and specialism, related party<br>- Commodities (consider sanctions)<br>- Esoteric, unusual or difficult to value assets<br>- Does fund accept in specie transfers<br>- Is fund proposing to make loans? If so is it a significant portion of the fund? Is the recipient a related party? Has the recipient been identified and verified? |
| d. Leverage and Borrowing (consider requirements under para 12 (7) of the Code) | - Is the lender regulated<br>- Source of wealth of the loan provision<br>- Jurisdiction<br>- Related party<br>- Financing fees and parties involved<br>- Reasons to borrow and reasons to lend<br>- Borrowing from related parties<br>- Borrowing is in the fund structure but may not be directly with the fund |
| e. Liquidity | - Liquidity of the asset |
| f. Unusual Features | - Understand the reasons for the features and how they could be abused<br>- This could relate to the product, the service providers or the assets |
| g. Target Market/ investors | - Jurisdiction and profile<br>- Private arrangements<br>- Specialist Investors<br>- Retail investors<br>- PEPs<br>- Sanctions<br>- Large single source of investment/transfer from another (related) structure<br>- Platforms |
| h. Distribution methods | - Financial Adviser (regulated/unregulated)<br>- Terms of business and reliance on others<br>- Website (global reach) |

| | |
|---|---|
| | - Jurisdictions |
| i. Governing Body | - Regulated / unregulated<br>- Track record – other funds (any that may have become insolvent) and experience in the fund's investment objective<br>- Integrity of board members (director of insolvent companies, disciplinary and regulatory action)<br>- Jurisdiction of domicile and residence of board members<br>- PEPs<br>- Sanctions<br>- Negative screening<br>- Any other relevant information |
| j. Sponsor/ Promoter &<br>k. Management Shareholder | - Regulated / unregulated<br>- Track record – other funds and in the fund's investment objective<br>- Jurisdiction of domicile and residence<br>- PEPs<br>- Sanctions<br>- Negative screening<br>- Any other relevant information |
| l. Regulated Functionaries | - Risks to arrangements<br>- Ownership/control<br>- Track record<br>- Jurisdiction<br>- PEPs<br>- Sanctions<br>- Reputation<br>- Negative screening<br>- Any other relevant information |
| m. Non - Regulated Functionaries | - Oversight of core functions<br>- Risks to arrangements<br>- Ownership/control<br>- Track record<br>- Jurisdiction<br>- PEPs<br>- Sanctions<br>- Reputation<br>- Negative screening<br>- Any other relevant information |
| n. Investment Committee | - Regulated / unregulated<br>- Track record<br>- Jurisdiction of domicile and residence of members<br>- PEPs<br>- Sanctions<br>- Any other relevant information |
| o. Other Influential Persons | - Regular suppliers and regular payments to non-functionaries<br>- Independence, potential conflicts of interest<br>- Risks to arrangements<br>- Track record<br>- Jurisdiction of domicile and residence<br>- PEPs<br>- Sanctions<br>- Any other relevant information |

| | |
|---|---|
| p. Conflicts of Interest | - Consider parties having more than 1 role and related parties<br>- Cross jurisdictional issues and risks<br>- Assets transferred to related party structures |
| q. Fund Rationale | - Does the rationale make economic sense |

### 5.4 Ongoing monitoring of the fund (customer)

The relevant person must perform ongoing and effective monitoring of any business relationship as per paragraph 13 of the Code and regularly review risk assessments (details of the review should be documented) and if appropriate these should be amended/updated as necessary. Some examples of potential higher risk indicators that may be flagged during the review process or ongoing monitoring of the fund customer are as follows (this is not an exhaustive list):

- entered into finance arrangements at a higher or lower rate than expected;
- no independent valuation of assets;
- payments away to connected parties or to unregulated third parties with no rationale;
- nature of assets changing;
- structure becomes more complex;
- purchase of assets no proof of title held by the administrator or the custodian;
- frequent changes of advisors/functionaries;
- transactions that result in big losses or total forfeiture;
- high fees paid to advisors/functionaries;
- conflicts of interest identified that are not being addressed by the fund; and
- jurisdiction of assets or investors changed to be higher risk

The relevant person should also consider the factors listed at 5.1 when performing ongoing monitoring.

## 6. Transfer of administration of a fund to another functionary

### 6.1 Customer (investor) due diligence

Where a relevant person (for this purpose the “successor firm”) is taking on the administration of an existing fund from another administrator (“predecessor firm”), the successor firm should take reasonable measures to ensure that the necessary CDD of the customers of the fund (the investors) has been undertaken on behalf of the fund prior to taking on the administration.

It may be possible to rely on the CDD (including evidence of identity) obtained by the predecessor firm (who is regulated in an equivalent jurisdiction) providing that the original CDD or certified copies of the original CDD is transferred to the successor firm as part of the fund’s records. The successor firm should assess the quality of the CDD (including evidence of identity held on the investors) and document deficiencies. Where there is insufficient evidence to support compliance with the Code then it may be appropriate for the successor firm, under delegation from the fund, to supplement the CDD with additional evidence to

meet the standards required by the Code. Further, if necessary, a remediation plan should be discussed with the fund and implemented as soon as is practicable after the transfer of administration. If deficiencies are serious, or the remediation plan will be protracted, the Authority should be notified.

## 6.2. Customer (investor) risk assessments

The successor firm will need to understand the arrangements being made by the fund in respect of the risk assessments of the investors (being customers of the fund whose administration is being transferred), and whether such risk assessments will be transferred to the successor firm (as they may form part of the fund's records) alongside the CDD (see 6.1).

If the risk assessments are able to be transferred to the successor firm, the successor firm is likely to, over time, update these risk assessments (as part its ongoing monitoring) based on its own policies and procedures, under delegation from the fund. If the successor firm finds deficiencies in the risk assessments they should discuss this with the fund and put in place a plan to remediate.

If the risk assessments are not able to be transferred to the successor firm, as part of the fund's records, a plan should be discussed with the fund and implemented as soon as is practicable after the transfer of administration.

If deficiencies are serious or any remediation plans will be protracted, the Authority should be notified.