



**ISLE OF MAN
FINANCIAL SERVICES AUTHORITY**

Lught-Reill Shirveishyn Argidoil Ellan Vannin

**Private Pensions
Sector Specific AML/CFT Guidance Notes
November 2021**

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/CFT Division
Financial Services Authority
PO Box 58,
Finch Hill House,
Bucks Road,
Douglas
Isle of Man
IM99 1DT

Tel: 01624 646000

Website: www.iomfsa.im

Email: aml@iomfsa.im

Version 2
(Last issued November 2021)

Contents

1. Foreword.....	4
2. Introduction	4
2.1 National Risk Assessment.....	4
2.2 Context of the sector.....	5
3. Risk guidance	5
3.1 Customer risk assessment.....	6
3.2 General higher risk indicators	7
3.3 Red flags	8
4. Customer due diligence and ongoing monitoring	9
4.1 Identifying the customer.....	9
4.2 Use of the concession at paragraph 21(1)	10
4.3 Payment of benefits from a scheme	11
4.4 Source of funds and the lifecycle of a pension scheme	12
4.5 Ongoing monitoring	12

Version history

Version 2 (November 2021)	<p>Updates to reflect changes to the main structure of the AML/CFT Handbook</p> <p>Removal of hyperlinks from footnotes to instead include hyperlinks in the main body for consistency purposes</p> <p>Amendments throughout to ensure consistency across all sector specific guidance documents</p> <p>Removal of table detailing different types of scheme, considered no longer appropriate for this document – new table to go into the amended Supplemental Information Document</p> <p>2.1 Includes up-to-date reference for the Island’s National Risk Assessment</p> <p>2.2 Further clarification regarding role of trustees and administrator</p> <p>3.1 Consolidation of higher risk factors into one list depending on type of scheme</p> <p>3.3 Section on “red flags” added</p> <p>4.1 Guidance amended in relation to who may be a customer in order to make more risk based</p> <p>4.2 Removal of detail regarding treatment of pension scheme if they are a customer of another relevant person, this is surplus to requirements as covered by section 4 of the Handbook</p> <p>4.3 Further detail inserted regarding paragraph 12(7) of the Code - included to provide additional clarification on the steps</p>
---------------------------	---

	required on payments of benefit out from a scheme
--	---

1. Foreword

For the purposes of this sector guidance, private pension schemes refer to retirement benefits schemes operated in or from the Isle of Man which are required to be registered as authorised schemes in accordance with the [Retirement Benefits Schemes Act 2000](#) (“the Act”).

2. Introduction

The purpose of this document is to provide guidance specifically for the private pensions sector in relation to anti-money laundering and countering the financing of terrorism (“AML/CFT”). This document should be read in conjunction with [the Anti-Money Laundering and Countering the Financing of Terrorism Code 2019](#) (“the Code”) and the main body of the [AML/CFT Handbook](#) (“the Handbook”).

Though the guidance in the Handbook and this sector 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 term is defined in paragraph 3 of the Code) regulatory/registered status as well as the fit and proper status of its owners and key staff, where appropriate.

This document covers unique money laundering and financing of terrorism (“ML/FT”) risks that may be faced by the sector and provides guidance in respect of customer due diligence (“CDD”) measures where a “one size fits all” approach may not work. Please see section 3 of this guidance for further details in relation to the risk profile of the sector.

2.1 National Risk Assessment

The Island’s [National Risk Assessment](#) (“NRA”) was published in 2015 and was updated in 2020.

The main ML vulnerabilities of private Isle of Man pension products tend to be found within personal schemes settled by members not resident in the Isle of Man with complex underlying investment structures or taxation arrangements; these may be vulnerable to the disguise of the proceeds of fraud and/or tax evasion. FT vulnerabilities tend to originate within large occupational schemes whose participating employers and employees/members are located around the world. The NRA sets out the main risks and vulnerabilities in detail.

Overall, after applying consideration of the product types and the controls and other preventative measures in place, the pensions sector is assessed in the NRA as having a medium low level of vulnerability for both ML and FT. The pensions sector must ensure that

its business risk assessment (and customer risk assessments where appropriate) takes into account any relevant findings of the NRA.

2.2 Context of the sector

There are several types of pension schemes operating in or from the Isle of Man to which the Code applies. These fall within two broad categories:

- domestic pension schemes - primarily available to Isle of Man residents; and
- international pension schemes - only available to persons resident and employed outside of the Isle of Man.

These are further sub-categorised as either a:

- personal scheme - for the provision of pension benefits to an individual; or
- occupational scheme - for the provision of pension benefits to the employees of an employer.

As the assets of these pension schemes must be held under irrevocable trust, the schemes must have appointed one or more trustees, who may be natural or legal persons. Schemes must also have an appointed retirement benefits schemes administrator (“Administrator”) who is responsible for the management of the scheme.

Schedule 4 of the [Proceeds of Crime Act 2008](#) designates both Administrators and Trustees¹, who carry out their duties for such pensions schemes by way of business, as relevant persons. In light of this, both the Administrators and the Trustees are subject to the Code requirements. Whilst the Authority acknowledges that in practice it is often the Administrator that undertakes some, or all, Code related compliance matters on behalf of a pension scheme and the Trustees; both the Trustees and the Administrator are relevant persons pursuant to the Code, as such it is the expectation of the Authority that both comply at all times with their respective obligations pursuant to the Code. In particular, Trustees and Administrators of such pension schemes must have due regard to the contents of paragraph 4(3) of the Code.

4 Procedures and controls

(3) the ultimate responsibility for ensuring compliance with this Code is that of the relevant person, regardless of any outsourcing or reliance on third parties during the process.

3. Risk guidance

The Code mandates that a number of risk assessments are completed –

¹ Trustees who are located outside of the Isle of Man are not in scope of the Code, however in order to undertake their duties appropriately it is expected they would have appropriate knowledge of the Code requirements. It is the responsibility of the trustee(s) to ensure the management of the scheme includes complying with any requirements in the jurisdiction in which they are located.

- a business risk assessment (“BRA”) (paragraph 5);
- a customer risk assessment (“CRA”) (paragraph 6); and
- a technology risk assessment (paragraph 7).

It is important for relevant persons to clearly differentiate between “business risk” and “customer risk” when undertaking the risk assessments:

- the BRA is an assessment of the ML/FT risks posed to the business by its environment, its customers, and the particular type of business model it operates; and
- the CRA is an assessment of the ML/FT risks posed by an individual customer to the business.

Further guidance regarding risk assessment requirements can be found in Chapter 2 of the Handbook.

The following provides an overview of some of the ML/FT risk indicators that may be seen in the differing pension schemes.

- Personal schemes:
 - sales channels and non-face-to-face business;
 - jurisdictional risks including bribery, corruption and tax evasion;
 - inappropriate use of pension schemes to access benefits prior to normal retirement (such as taking loans or early payments); and
 - arrangements where a scheme member has power to directly instruct on scheme investments, with insufficient trustee oversight.
- Occupational schemes:
 - interests/subsidiaries/participating employers or employees in multiple jurisdictions;
 - schemes established for fictitious employees;
 - sales channels;
 - complex taxation arrangements; and
 - FT and proliferation risks.

3.1 Customer risk assessment

As with the basic elements of a CRA discussed in chapter 2 of the Handbook, the following should be considered in all cases, as appropriate and on an ongoing basis:

- customer location;
- trustee location;
- Politically Exposed Person (“PEP”) status;
- source of funds and/or source of wealth – in particular in relation to contributions ensuring activity seems commensurate with knowledge of the relationship – see paragraphs 8 and 15 of the Code and section 3.8 of the Handbook;
- sales channels - in particular where unregulated advice may have been provided;

- unregulated or unrecognisable investments and loans from the scheme;
- connected parties – their funding responsibilities and status;
- multi-jurisdictional arrangements and regulatory arbitrage;
- third party payments – see Code requirements at paragraph 12;
- rapid turnaround/divestment;
- activity on underlying assets – where a scheme member or beneficiary has direct access to or control over any scheme assets without adequate trustee oversight;
- weak administrative controls;
- scheme type such as international end of service gratuity or statutorily prescribed savings plans; and
- reliance on a previous pension scheme administrator or trustee for source of wealth information (where a transfer from another pension scheme is used to fund the member's benefits in the scheme).

3.2 General higher risk indicators

The following activities may be indicative of increased risk:

- conflicted trustees and/or directors of an administrator;
- large cash sums deposited into a scheme by a member, particularly when followed by substantial withdrawal of funds;
- deposit of securities or other assets, whose origin or ownership is unclear;
- transfer of assets from an unidentified third party into a scheme;
- a third party making cash contributions into a scheme;
- transferring of securities or other assets into a scheme which would not normally be allowed under statutory or scheme rules; and/or
- unemployed persons paying contributions into a scheme.

Just because an activity / scenario is listed above it does not automatically make the relationship higher risk. The customer's rationale and the nature /intended purpose of the business relationship and any controls that are in place should be considered in all cases. Also, a list of suggested red flags is included at section 3.3 of this document.

Paragraph 15(5) of the Code mandates certain circumstances where a customer must be rated as higher risk. Apart from these matters, the Authority does not generally mandate which customer or sectors must be viewed as higher risk. The Authority has no objection to a relevant person having higher risk customers provided those customers have been adequately risk rated in accordance with the relevant person's procedures and any mitigating factors have been documented. As per paragraph 15(3) of the Code a relevant person must conduct enhanced due diligence where a customer has been assessed as posing a higher risk.

If a satisfactory explanation from a customer is not received in the event of any situations, features, or activities which cause concerns, it should be determined whether this may be suspicious or unusual activity. 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 enhanced customer due diligence 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 enhanced customer due diligence in accordance with paragraph 15 of the Code, unless the relevant person believes conducting enhanced customer due diligence will tip off the customer; and
- (b) make an internal disclosure.

3.3 Red flags

In addition to the higher risk indicators noted above, there are some factors that are likely to be “red flags” in relation to that particular relationship and would therefore usually be considered suspicious activity. If a relevant person identifies suspicious activity, appropriate steps as explained in section 3.2 of this document, and paragraph 13 the Code, must be taken. An indicative list of some red flags is given below, but this list is by no means exhaustive:

- where a customer provides false or misleading information and / or tries to conceal their identity;
- where a customer provides suspicious identification documents;
- where 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 activity;
- where a customer is secretive / evasive when asked to provide more information;
- the customer refuses to identify a legitimate source of funds or source of wealth;
- where a customer refuses to provide details of beneficial owners or provides information which is false, misleading or substantially incorrect;
- where a customer enquires about how quickly they can end a business relationship where it is not expected and with no rationale;
- where the business relationship is ended unexpectedly by a customer and the customer accepts unusually high fees to terminate the relationship without question;
- the customer appears to be acting on behalf of someone else and does not provide satisfactory information regarding whom they are acting for;
- where a 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

- where a customer requests paying higher charges to keep their identity secret.

4. Customer due diligence and ongoing monitoring

Part 4 of the Code requires relevant persons to undertake customer due diligence and ongoing monitoring in relation to all business relationships.

Chapter 3 of the Handbook provides guidance on how to identify and verify the identity of the customer. Additionally, in order to determine the customer due diligence and ongoing monitoring requirements of a scheme during its lifetime, the relevant person will, as a minimum, need to consider the following matters:

- the type of scheme (International, Domestic, Personal, Occupational);
- the source of any funds being transferred/paid into a scheme – as per paragraph 8(3)(e) of the Code;
- the destination of any funds being paid out of the scheme – as per paragraph 12(7) of the Code (see section 4.3 of this document);
- any significant events taking place during the lifetime of a scheme and any conditions attaching to benefits due;
- who is establishing the scheme and whether any other person, natural or legal, may pay funds into or have significant control over the assets of the scheme; and
- whether payments from a scheme may be due to any person(s) other than a scheme member, and the rationale for this arrangement.

In all cases where the requirements of Part 4 of the Code cannot be met (Paragraphs 8(5), 9(9), 10(5), 12(11), 14(6), 15(8) and 19(11)) the relevant person's procedures and controls must provide that –

- (a) the business relationship must proceed no further;
- (b) the relevant person must consider terminating the business relationship; and
- (c) the relevant person must consider making an internal disclosure.

4.1 Identifying the customer

Paragraph 8(2) of the Code requires a relevant person to undertake procedures and controls in relation to new business relationships:

8 New business relationships

- (2) Subject to sub-paragraph (4), the procedures and controls must be undertaken -
 - (a) before a business relationship is entered into; or
 - (b) during the formation of that relationship.
- (3) Those procedures and controls are –
 - (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) taking reasonable measures to establish the source of funds including, where 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.

Typically a customer would normally include any person legal or natural who transfers/settles / contributes or pays funds into the pension scheme. Examples of factors to consider in order to assist in identifying a customer include the below.

- Who is establishing the scheme?
- Who is controlling the business relationship?
- With which parties are there contractual agreements?
- Who is funding the business relationship?

It is important to note that such list of factors is not exhaustive.

A scheme will often have more than one connected party depending on its specific fact-pattern. Parties to a scheme commonly change over time or upon the occurrence of significant events such as the addition or death of a member, a change or addition of an employer or, in certain circumstances, an alteration to the deed or rules of a scheme.

It is also important to note the contents of paragraph 21(1) of the Code covered further below.

4.2 Use of the concession at paragraph 21(1)

Paragraph 21(1) of the Code states:

21 Miscellaneous

In respect of a pension, superannuation or similar scheme that provides retirement benefits to employees, if contributions are made by way of deduction from wages and the scheme rules do not permit the assignment of a member's interest under the scheme, the relevant person –

- (a) may treat the employer, trustee or any other person who has control over the business relationship, including the administrator or the scheme manager, as the customer; and
- (b) need not comply with paragraph 12(2)(b).

Where the requirements of this paragraph are met and whilst the pension benefit is not in payment but continues to accrue, the Administrator may treat the employer or Trustee (as appropriate) as the customer for Code requirements in relation to customer risk assessment, customer due diligence and ongoing monitoring.

Where contributions are made by a “main” employer and other participating companies within the corporate group, though the “main” employer may be seen as the ‘customer’, appropriate risk assessment, due diligence and AML/CFT considerations may still need to be applied on the participating companies as they may offer different risk profiles to that of the main employer.

Where a payment is to be made out of the scheme to an employee/member or third party, it is important to note that paragraph 12(7) of the Code applies in all circumstances (see section 4.3).

4.3 Payment of benefits from a scheme

Where a scheme benefit is to be paid, the relevant person must consider what steps are required to authorise and execute the payment; this consideration must be done on a case-by-case basis and in respect of each payment made from the scheme. The purpose of appropriate checks on payout is to mitigate potential risks of ML/FT including sanctions breaches as well as ensuring the payment is going to the intended recipient.

A relevant person must demonstrate compliance with paragraph 12(7)² of the Code by identifying and, on the basis of materiality and risk, verifying the identity of any person who is a recipient/beneficiary of a payment from a scheme. Further, it is the Authority’s expectation that a relevant person undertakes checks to determine whether the payment recipient/beneficiary is listed on a sanctions list prior to any payment being made.

12 Beneficial ownership and control

(7) Subject to paragraph 21(1) and without limiting sub-paragraphs (2) to (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

² This Code requirement derives from FATF recommendation 10 which states “for life or other investment related insurance type businesses, financial institutions should, in addition to the CDD measures required for the customer and the beneficial owner, conduct CDD on the recipients/beneficiaries of insurance or investment products including pensions. This includes verification of the identity of the recipients/beneficiaries at the time of the payout.”

It is important to note that a relevant person's procedures must be clear in relation to the steps to be taken on payments being made out of a scheme, and the procedures should demonstrate that such relevant person has appropriately considered the BRA and CRA when determining the approach in this area.

Paragraph 12(7) of the Code should be read in conjunction with paragraph 21(1) of the Code, where this latter paragraph applies. For the avoidance of any doubt, it should be noted that paragraph 21(1) explains who can be treated as a customer for the purposes of a pension scheme, it does not disapply paragraph 12(7) of the Code.

Where there are higher risk indicators, it must be considered whether enhanced due diligence is required as per paragraph 15 of the Code. If there are any suspicious circumstances, appropriate action must be taken as set out in section 3.2 above.

4.4 Source of funds and the lifecycle of a pension scheme

There are a number of different pension schemes with a variety of funding arrangements which may change throughout the life of the scheme. Relevant persons are required to ensure that they carry out appropriate due diligence on all funds being paid into a scheme as well as ensuring that they can identify the relevant parties to the scheme at all times. Please see section 3.8 of the Handbook for further details on what information should be established in respect of source of funds and source of wealth.

4.5 Ongoing monitoring

The guidance provided in chapter 3 of the Handbook should be considered and, wherever possible and appropriate, followed when conducting ongoing monitoring in this sector. As noted above, there are a number of changes which may occur during the lifecycle of a pension scheme in respect of customer(s) and source of funds. These changes must be monitored and reviewed, each review must be documented, and where appropriate, the customer risk assessment amended, with documentation produced and retained in accordance with the requirements set out in the Code.