ISLE OF MAN
FINANCIAL SERVICES AUTHORITY

Lught-Reill Shirveishyn Argidoil Ellan Vannin

Anti-Money Laundering and Countering the Financing of Terrorism Handbook

~~December 2023~~February 2025

Version history

Version 1 (July 2021)	First version of the current Handbook created.
Version 2 (December 2023)	Throughout document – minor typographical errors amended and hyperlinks updated where appropriate. Section 1.4 – Updated document to remind relevant persons licensed under the Financial Services Act 2008 of their reporting obligation under Rule 8.17 of the Financial Services Rule Book 2016. Section 2.2.7 – Emphasis added that the BRA must be evidenced at all times and a version history should be maintained in order to demonstrate compliance with the Code. Section 2.2.8 – Clarification added that the BRA should be a living document. Section 2.2.8.1 – Emphasis added that the BRA must evidence the relevant person has assessed the risk of ML/FT posed by the business and customers and that it considers all risk factors detailed in the Code. Section 2.2.8.2 – Emphasis added that the BRA must be documented and recorded. Section 2.2.8.3 – Emphasis added that the BRA must consider the Island's latest NRA and the impact this may have on the relevant person's business. Section 2.2.9 – Section updated to reflect the requirement to undertake a customer risk assessment for each of the relevant person's customers. In addition, the BRA should reference the relevant person's customer base. Section 2.2.9 – Clarity added that a documented CRA is required for all customers. Section also updated to reflect it is prudent for relevant persons to start from a position of higher risk and mitigate risk factors accordingly as the CRA is undertaken. Section 2.2.9.2 – A footnote added to cross reference to the TCSP AML/CFT/CPF Sector Specific Guidance. Section 3.4.3 – Further clarification added to assist firm's with understanding of the introduced business provisions. Section 3.4.3.1 – New section added to further explain the concept of "introduced business".

	Section 3.3.4.2 – Tweaks made to the diagram, which assists relevant persons determining if there is an introduced business relationship. Section 3.4.5.4 – Footnote added to confirm that appropriate procedures and controls must be in place to ensure the recipient or beneficiary of a loan is not on a sanctions list. Section 3.5.1 – Clarification issued regarding the customer information required from the Proceeds of Crime (Prescribed Disclosures) Order 2015. Section 3.8.10.3 – Further detail added to cover circumstances in which SOW of a PEP may not need to be established. Section 4 – Clarification added to advise that the relevant person should ensure a record is kept off what concessions are used in what cases as this will assist with their own risk assessments and aid with completion of the Authority's AML/CFT/CPF Statistical return. Section 5.1 – Detail about FIU initiative regarding Public Private Partnerships ("PPPs") added. Section 5.3.1 – Hyperlink to additional FIU Guidance note added. Section 6.1 – Updated to reflect the expectations by firms licensed under the Financial Services Act 2008 and Insurance Act 2008 of meeting Paragraph 30 of the Code
Version 3 (February 2025)	Section 1 - Guidance now colour coded to differentiate between where different regulations and legislation and being referred to. Section 2.2.9 – Updates made to the Customer Risk Assessment guidance to provide additional clarity. Section 2.2.9.2 – additional information has been added in relation to Commercially Exposed Persons (CEPs). Section 3.4.6.6 – Updates to guidance around the extent of ongoing monitoring to make it explicit that consideration should be given, where necessary, to SOF and SOW information when undertaking in ongoing monitoring and periodic reviews. Throughout document – any minor typographical errors amended and hyperlinks updated where appropriate. Split out terminology for Money Laundering (ML), Terrorist Financing (TF) and Proliferation Financing (PF) for additional clarity.

Contents

1. Introductory

Colour code used within this guidance to refer to other regulation and legislation.

AML/CFT Code 2019

AML/CFT (Civil Penalties Regulations) 2019

DBROA 2015

POCA 2008

1.1 Purpose and scope

The purpose of the Anti-Money Laundering and Countering the Financing of Terrorism ("AML/CFT") Handbook "the Handbook" is to assist relevant persons supervised or overseen for AML/CFT/CPF purposes by the Isle of Man Financial Services Authority ("the Authority") to understand and satisfy their obligations under the Anti-Money Laundering and Countering the Financing of Terrorism Code 2019 ("the Code"). The Code can be found at the Isle of Man Government's legislation website.

Other competent authorities[1] have also produced guidance on particular AML/CFT/CPF requirements where those matters fall within their responsibilities. This Handbook is complementary to and does not supersede the guidance issued by other competent authorities.

The competent authority in relation to the disclosure of ML/FT/PF suspicions is the Isle of Man Financial Intelligence Unit ("the IOMFIU"). The IOMFIU's document

[1] Defined in paragraph 3(1) of the Code as all Isle of Man administrative or law enforcement authorities concerned with AML/CFT, including in particular the Isle of Man Financial Services Authority, the Isle of Man Gambling Supervision Commission, the Department of Home Affairs, the Economic Crime Unit of the Isle of Man Constabulary, the Financial Intelligence Unit, the Office of Fair Trading, the Attorney General and the Customs and Excise and Income Tax Divisions of the Treasury.

Guidance for making Suspicious Activity Reports (and Other Disclosures) to the Financial Intelligence Unit ("IOMFIU Guidance") is the primary guidance on that subject.

The competent authority in relation to the administration of United Nations and UK financial and trade sanctions and export licensing controls in the Isle of Man is the Isle of Man Customs and ~~Excise~~Immigration Division ("IOMCI") ~~("IOMCE").~~ The ~~IOMCE's~~IOMCI's website provides information and the Island's primary guidance on:

- financial sanctions;
- current sanctions regimes;
- terrorism and terrorist financing;
- proliferation and proliferation financing;
- export control and trade control; and
- trade based money laundering.

This Handbook takes a multilevel approach:

1) Guidance sets out the Authority's expectations for meeting the requirements of the Code. The guidance should be read in conjunction with, and not in isolation from, the Code, other AML/CFT/CPF legislation and guidance issued by other competent authorities.

2) Sector specific guidance documents are provided to emphasise particular ML/FT/PF risks of certain products and services offered by relevant persons in particular sectors, and to refine guidance on CDD measures according to those risks. These documents should be read in conjunction with the main guidance.

3) The Supplemental Information Document that provides suggestions on specific AML/CFT requirements is provided for relevant persons requiring further assistance. This document is not considered by the Authority to be guidance as per paragraph 42(2) of the Code. Where relevant persons make use of the suggestions, they should only do so in conjunction with, and not in isolation from the Code, other AML/CFT/CPF legislation, the main guidance and sector specific guidance.

This Handbook is not exhaustive, nor does it set limitations on the steps relevant persons must take to meet their AML/CFT/CPF obligations. It is not a proforma procedures manual nor a checklist of things that all relevant persons must do, or not do, in order to meet their AML/CFT/CPF obligations, and it must not be treated as such. Where lists or examples are provided, these are not exhaustive. The examples present some, but not the only ways relevant persons may meet their obligations. A reasonable, proportionate and intelligent risk based approach is required. Each relevant person must consider its own particular circumstances. This includes additional measures that it may be necessary to implement in order

to prevent its exploitation, and that of its products and services, by persons seeking to launder criminal property or to finance terrorism or the proliferation of weapons of mass destruction. It is a matter for each relevant person, based on their own particular circumstances, to ensure they comply with the AML/CFT/CPF legislation. Relevant persons must therefore make their own assessments of how they will meet their AML/CFT/CPF obligations.

For ease of reference, the Handbook contains extracts from relevant legislation which are boxed for clarity. However, these extracts must not be considered as a substitute for the original documents. References to relevant legislative provisions are also provided in the margin against related guidance. All Isle of Man primary legislation can be found here and all Isle of Man secondary legislation can be found here.

The Handbook does not provide extracts of, or guidance on, all of the Code provisions. This is because any such guidance would be superfluous.

If a term is defined in the Code the same definition applies in the Handbook. All abbreviations used in the Handbook, which are not otherwise used in the Code, are expanded in the Handbook's glossary. Should any inconsistencies occur between the text in the Handbook and the Code, the Code has primacy.

~~Relevant persons must note that where the term "financing of terrorism" or its abbreviation "FT" are used, they also include "the financing of proliferation" ("FP"). Accordingly where "countering the financing of terrorism" or "CFT" are used, they also include "countering the financing of proliferation" ("CFP").~~

The Handbook is not the only source of information on ML/FT/PF risks or on meeting AML/CFT/CPF obligations. Other sources include:

- the Isle of Man's National Risk Assessment published by the Cabinet Office, at the time of publishing this assessment is currently undergoing a wholesale revision;
- guidance and good practice provided by the IOMFIU on making suspicious activity reports;
- guidance issued by the ~~IOMCE~~IOMCI on Financial Sanctions, Terrorism and Terrorist Financing, Proliferation and Proliferation Financing and Trade Based Money Laundering;
- guidance issued by the Financial Action Task Force ("FATF") on Money Laundering/ Financing of Terrorism and Proliferation risk as well as topical and sectoral guidance;
- guidelines on AML/CFT/CPF matters including on CDD issued by the Bank for International Settlements Basel Committee on Banking Supervision; and
- guidelines on risk factors issued by the European Supervisory Authorities.

1.2 Legislative framework

The FATF is the AML/CFT/CPF global standard setting body and its Recommendations are recognised as the global AML/CFT/CPF standards against which all jurisdictions are assessed for compliance.

The Isle of Man's AML/CFT/CPF framework of legislation and guidance is drafted to meet the FATF AML/CFT standards. AML/CFT/CPF legislation as defined by the Code means:

- section 7 to 11 and 14 of the Anti-Terrorism and Crime Act 2003 ("ATCA");
- part 3 of the Proceeds of Crime Act 2008 ("POCA");
- parts 2 to 4 of the Terrorism and Other Crime (Financial Restrictions) Act 2014 ("TOCFRA");
- financial sanctions which have effect on the Island; and
- the Code.

~~All Isle of Man primary legislation can be found here and all Isle of Man secondary legislation can be found here.~~

POCA s157, TOCFRA s68

The Code is made under section 157 of POCA and section 68 of TOCFRA 2014 and applies to persons carrying on business in the regulated sector (referred to as "relevant persons") as set out at paragraph 2(6)(a) to (t) of Schedule 4 to POCA.

AML/CFT (Civil Penalties) Regulations 2019

The AML/CFT (Civil Penalties) Regulations 2019 are made under section 157 of POCA and section 68 of TOCFRA. These AML/CFT Civil Penalties Regulations specify the circumstances when the Authority may impose a civil penalty on a relevant person for contravention of the Code.

1.3 Data protection

Relevant persons must comply with the AML/CFT/CPF requirements having regard to their obligations under data protection legislation. Further information about data protection can be found on the Information Commissioner's website.

1.4 Status of the Handbook

FSA2008 s.2(2)(b), s.12

The guidance in this Handbook is issued under section 12 of the Financial Services Act 2008 ("FSA 2008") for the purpose of meeting the Authority's regulatory objective of "the reduction of financial crime". It is relevant to all sectors regulated by the Authority, including insurance and pensions.

DBROA 2015 s.32

The guidance in this Handbook is also issued under section 32 of the Designated Businesses (Registration and Oversight) Act 2015 ("DBROA 2015") which enables the Authority to provide guidance on AML/CFT/CPF legislation for designated businesses.

The Handbook also derives status from AML/CFT/CPF legislation, including the Code.

POCA 142(12), 143(10), ATCA 14(6), TOCFRA 36(4), 39(3), Code 42(2), AML/CFT (Civil Penalties Regulations 2019 5(2)(j), IA 2008

The Handbook's guidance is neither legislation nor is it legal advice. However, it is persuasive in respect of breaches of the Code and potentially in respect of other AML/CFT/CPF legislation (as per the references provided). Where a relevant person follows guidance this would indicate compliance with associated legislative provisions and vice versa. For the avoidance of doubt, this guidance does not constitute binding guidance under the Insurance Act 2008 ("IA 2008").

The Handbook's guidance is relevant whether breaches of the Code are dealt with either criminally, civilly by way of civil penalties, or in respect of the Authority's considerations of a relevant person's regulatory / registered status and the fit and proper status of its owners and key staff where appropriate. Relevant persons should be aware that in some cases a decision making body (whether the Court, the Treasury or the Authority) may take account of guidance issued by the Authority, in other cases, it must consider whether the guidance was followed.

The Code provides:

Code 42

42 Offences

(2) In determining whether a person has complied with any of the requirements of the Code, a court may take account of –

(a) any relevant supervisory or regulatory guidance given by a competent authority that applies to that person;

The AML/CFT (Civil Penalties) Regulations 2019 provides:

AML/CFT (Civil Penalties Regulations 2019 5(2)(j)

5 Civil Penalties

(2) In determining whether to impose a penalty under paragraph (1) the Authority shall have regard to factors such as –

(j) compliance with any relevant supervisory or regulatory guidance provided by a competent authority that applies to the relevant person;

The DBROA 2015 provides:

DBROA 2015 32(6)

32 Guidance

(6) In any proceedings under this Act or otherwise, any guidance issued under this section is admissible in evidence if it appears to the court or tribunal conducting the proceedings to be relevant to any question arising in the proceedings, and must be taken into account in determining any such question.

The level of a relevant person's compliance with AML/CFT/CPF legislation directly affects its licensed, authorised or registered status as well the fit and proper

status of those individuals holding certain positions or roles. The Authority will take account of the Handbook's guidance when assessing the level of compliance with AML/CFT/CPF legislation.

Nothing in the Handbook should be read as providing an express or implied assurance that the Authority would defer or refrain from using its powers where a suspected contraventions of the AML/CFT/CPF legislation comes to its attention.

Relevant persons must always refer directly to the AML/CFT/CPF legislation when determining their legal obligations. The Handbook does not replace or override any legal and/or regulatory requirements. In the event of a discrepancy between the Handbook and the AML/CFT/CPF legislation, the AML/CFT/CPF legislation takes precedence.

The Handbook is not legal advice. Where relevant persons are unsure about the application of the AML/CFT/CPF legislation to their particular circumstances, they should seek legal advice.

Relevant persons that are licensed under the Financial Services Act 2008 are subject to the Financial Services Rule Book 2016 and therefore must be cognisant of Rule 8.17 (Breaches of regulatory requirements) and ensure if a contravention of the Code is identified the appropriate notification under the Rule is provided. The Authority's briefing document on materiality of rule breaches is available here.

1.5 What is money laundering, financing of terrorism and the financing of proliferation?

Code 3(1), POCA s.158, 139, 140, 141, 181, 198
ATCA s.7, 8, 9, 9A, 10
TOCFRA s.3

Definitions pertaining to, and the offences of, money laundering, financing of terrorism and financing of proliferation in the Isle of Man context are found within the Code, POCA, ATCA and TOCFRA. Relevant persons must refer to the full legal documents to ensure full context, understanding and compliance.

It is important that relevant persons have an in depth understanding of what money laundering, financing of terrorism and financing of proliferation involves and how it may present to their organisations. The NRA will assist with this understanding, as will guidance issued by ~~IOMCE~~IOMCI on terrorism, financing of terrorism, proliferation, the financing of proliferation and trade based money laundering which can be found on their website. The FATF, as the international standard setting body in this area, has a number of documents on their website which will assist relevant persons in developing their understanding and keep up to date with developments in these areas.

2. General requirements and risk based approach

2.1 General requirements

2.1.1 Inclusion of countering the financing of proliferation within AML/CFT/CPF requirements

Code 3(1) Relevant persons must note that the Code's requirements apply in respect of countering the financing of proliferation as well as in respect of countering money laundering and the financing of terrorism. This is also the case in this Handbook if not otherwise explicit.

> **3 Interpretation**
>
> (1) In this Code -
>
> **"financing of terrorism"** includes the financing of proliferation and is to be construed in accordance with the definitions of **"financing"**, **"terrorism"** and **"proliferation"** in section 3 of the Terrorism and Other Crime (Financial Restrictions) Act 2014;

2.1.2 Procedures and controls

Code 4(1) The Code makes clear that before any business is conducted for a customer or another person, a relevant person must have in place specified procedures and controls.

These procedures and controls are vital to help protect the relevant person, their staff, their business and their communities from the threat of being used or abused by criminals or those assisting or enabling criminals. Relevant persons must demonstrate they are protecting themselves in order to make their domain as hostile as possible to those who would abuse them. In this way, the procedures and controls are vital for the effective prevention of ML/FT/PF and the harm that crime, terrorism and the proliferation of weapons of mass destruction present for wider society.

Code 3(1)

3 Interpretation

(1) In this Code -

"AML/CFT" means anti-money laundering and countering the financing of terrorism;

"AML/CFT legislation" means the requirements of –

(a) sections 7 to 11 and 14 of the Anti-Terrorism and Crime Act 2003;
(b) Part 3 of the Proceeds of Crime Act 2008;
(c) Parts 2 to 4 of the Terrorism and Other Crimes (Financial Restrictions) Act 2014;
(d) financial sanctions which have effect in the Island; and
(e) this Code,

Code 4(1)(a)

4 Procedures and controls

(1) A relevant person must not enter into or carry on a business relationship, or carry out an occasional transaction, with or for a customer or another person unless the relevant person -

(a) establishes, records, operates and maintains procedures and controls –

(i) in order to comply with each paragraph within Parts 3 to 9;

(ii) in relation to determining whether a customer, any beneficial owner, beneficiary, introducer or eligible introducer is included on the sanctions list; and

(iii) in relation to internal controls and communication matters that are appropriate for the purposes of forestalling and preventing ML/FT;

The procedures established must all be in writing. It is not acceptable for any of the procedures to be undocumented practices or customs. Without documentation, procedures can become confused and the purpose and rationale behind them can become lost such that they are no longer followed.

These documented procedures must be understandable and appropriately accessible to all those conducting business on behalf of the relevant person in order to ensure they can be followed and standards maintained. Whether procedures and controls are available to staff electronically or in hard copy is a matter for relevant persons to determine based on their own communication practices and needs.

Relevant persons must ensure that the procedures and controls they have established are operated consistently. It is recognised that there may be circumstances when necessary but unforeseen or unplanned deviations from the procedures and controls may occur. Relevant persons should have procedures and controls in place to deal with these circumstances, ensuring that any deviations are subject to reasoned assessment of the ML/FT/PF risks and relevant approvals where relevant persons are satisfied they can manage those ML/FT/PF risks. The deviation, assessment, rationale and approval should be fully documented both as

regards the case involved and subsequently as part of updating the relevant person's documented procedures and controls.

Code 30

Relevant persons must maintain these procedures, ensuring that they remain fit for purpose. This will involve reviewing and testing the procedures to ensure they remain effective, continue to enable the relevant person to manage and mitigate their ML/FT/PF risks and are in line with current AML/CFT/CPF legislative requirements. Deviations from the normal procedures and controls will form part of such reviews. Relevant persons must always be aware that the overarching aim for any AML/CFT/CPF procedures and controls is to prevent ML/FT/PF, ultimately reducing harm to society.

See section 6.1 for guidance on paragraph 30 of the Code which deals with monitoring and testing compliance with AML/CFT/CPF legislation.

Relevant persons should also ensure that their procedures for developing, documenting and maintaining their AML/CFT/CPF procedures and controls are robust.

Code 4(1)(b)

4 Procedures and controls

(1) A relevant person must not enter into or carry on a business relationship, or carry out an occasional transaction, with or for a customer or another person unless the relevant person -

(b) takes appropriate measures for the purpose of making its employees and workers aware of –

(i) the AML/CFT legislation; and

(ii) the procedures and controls established, recorded, maintained and operated under head (a).

Code 4(1)(b), 32

Guidance on staff training in respect of paragraphs 4(1)(b) and 32 is in section 6.3.

Code 4(2)(c)

4 Procedures and controls

(2) The procedures and controls referred to in sub-paragraph (1) must –

(c) be approved by the senior management of the relevant person.

Code 3(1)

3 Interpretation

(1) In this Code -

"senior management" means the directors and officers or any other persons who are nominated to ensure that the relevant person is effectively controlled on a day-to-day basis and who have responsibility for overseeing the relevant person's proper conduct;

Code 4(2)

Senior management approvals should be comprehensively documented such that it is clear what procedures and controls are approved each time, as well as any

considerations, analysis and rationale relevant to the approval. This is particularly important as a consequence of the requirement for risk based procedures and controls.

See section 2.2.2 for guidance on the risk based approach.

Code 4(3)

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.

Code 4(3), 42

Though it may be possible to place reliance on specified third parties or outsource certain AML/CFT/CPF practices to others, it is not possible to outsource responsibility for compliance with any of the Code's requirements. The offences at paragraph 42 of the Code apply to the relevant person and any officer or partner (where relevant) where the relevant person has contravened the Code's requirements. Relevant persons should therefore ensure they are satisfied that, where they place reliance on a third party by whatever means, the requirements of the Code are met.

2.2 Risk Management

2.2.1 Definitions

The Code does not define "risk" or other related terms. Consequently, the following definitions are used in this handbook.

"Risk" means:

In the context of AML/CFT/CPF:

- **threats** to the relevant person from person(s), objects or activities with the potential to cause harm. It can be actual or a potential threat. Not all threats present the same risk level to all relevant persons;
- **vulnerabilities** within the relevant person that can be exploited by the threat or that may support or facilitate its activities; and
- **consequences** the impact and likelihood of ML/FT/PF taking place.

"Inherent risk" means the level of risk that exists before mitigation.

"Residual risk" means the level of risk that remains after mitigation.

"Risk appetite" means the type and level of risk a relevant person is prepared to accept.

"Risk factors" means variables that, either on their own or in combination, may increase or decrease the ML/FT/PF risk posed by an individual business relationship/occasional transaction.

"Risk based approach" means an approach where relevant persons identify, assess and understand the ML/FT ~~(including FP)~~/PF risks to which they are exposed and take AML/CFT/CPF measures that are proportionate to those risks.

"Mitigation" means implementing controls and procedures to reduce identified ML/FT/PF risks.

2.2.2 Risk based approach

The purpose of a risk based approach is for relevant persons to identify and assess the realistic ML/FT/PF risks they and their customers face, and to ensure they apply appropriate controls and procedures within their business and on their customers. This includes increased vigilance, and higher level or enhanced controls and management involvement where higher risks are involved. Minimum Code requirements still apply in cases where the relevant person has correctly assessed there is not a higher risk.

Code 4(2)

4 Procedures and Controls

(2) The procedures and controls referred to in sub-paragraph (1) must –

(a) have regard to the materiality and risk of ML/FT including whether a customer, beneficial owner, beneficiary, introducer or eligible introducer poses a higher risk of ML/FT;

(b) enable the relevant person to manage and mitigate the risks of ML/FT that have been identified by the relevant person when carrying out the requirements of the Code;

(c) be approved by the senior management of the relevant person.

Code 4(2), Parts 3 - 9

Taking a risk based approach is an overarching requirement by virtue of paragraph 4(2) and is fundamental to effectively implementing the Code's AML/CFT/CPF measures at Parts 3 to 9. This means that all of the procedures and controls required to be established by relevant persons including risk assessments, customer due diligence ("CDD"), compliance and record keeping as well as some miscellaneous requirements must be risk based.

Code 5

In order to ensure such procedures are appropriately risk based, relevant persons must identify, assess and understand the ML/FT/PF risks to which they are exposed based on a thorough review of available information. The business risk assessment ("BRA") is the starting point in this process. Relevant persons should tailor their procedures and controls to effectively manage and mitigate those risks.

2.2.2.1 A risk based approach is not a "zero failure" approach

In a risk based regime, not all relevant persons will adopt the same AML/CFT/CPF procedures and controls and relatively isolated incidents of insignificant risk should not necessarily invalidate the integrity of a relevant person's AML/CFT/CPF procedures and controls. Conversely, a flexible risk based approach does not exempt relevant persons from applying effective AML/CFT/CPF procedures and

controls. Relevant persons should be able to explain the effectiveness of their AML/CFT/CPF procedures and controls and how those procedures and controls are commensurate to the risks identified.

Relevant persons should always strive to detect and prevent ML/FT/PF. Though it is recognised that resources are not infinite, they should be commensurate with the AML/CFT/CPF need. A risk based approach is not, however, a "zero failure" approach. Consequently, there may be occasions where a relevant person has taken all reasonable measures to identify, assess and mitigate ML/FT/PF risks, but it is still used for ML/FT/PF purposes in isolated instances.

2.2.2.2 Useful information sources for developing a risk based approach

The FATF has issued guidance on the risk based approach for a number of sectors which relevant persons may find helpful.

The European Supervisory Authorities have issued guidelines on ML/FT/PF risk factors which are applicable within the European Union ("the EU"). These guidelines are not binding on the Isle of Man as a non-EU jurisdiction, though relevant persons may find them helpful.

2.2.3 Risk assessments

Code 4(1), (2), 5, 6, 7, 9(3), (4), 19(4)(g)

Relevant persons must ensure they have a thorough understanding of the ML/FT/PF risks they are exposed to. To this end, relevant persons must establish procedures and controls for BRA, customer ("CRA") and technology risk assessments ("TRAs"), which must be recorded. The relevant person must operate these procedures and controls, meaning they must undertake the relevant risk assessments according to those procedures. Relevant persons must also maintain their risk assessment procedures to ensure they remain effective and up to date enabling the relevant person to manage and mitigate their ML/FT/PF risks. This involves reviewing their procedures and documenting updates to those procedures as well as capturing the rationale for any variations from it. Such procedures and controls must be risk based meaning they should be tailored and proportionate to the relevant person's particular circumstances. In addition, the procedures and controls must be approved by the relevant person's senior management.

When assessing ML/FT/PF risk, relevant persons should analyse and seek to understand how the ML/FT/PF risks they identify affect their business. This requires an understanding of the ML/FT/PF risk faced by the wider sector(s) as well as in respect of the relevant person's specific business and its customers.

Code 4(2), 5, 6, 7, 14, 15(3), 16 - 22

The BRA, CRA and TRAs are interconnected with each type of risk assessment informing the other. Furthermore, they are the vital base on which to determine a relevant person's risk appetite and build risk sensitive AML/CFT/CPF mitigation procedures and controls such as CDD procedures. Mitigation procedures and controls must flow from the results of the risk assessments, but equally information gained when operating mitigation procedures and controls such as for

CDD and monitoring should feedback into risk assessment considerations. Risk assessments and mitigation measures are in a continuous feedback loop. Mitigation procedures and controls must also be tailored according to relevant persons' particular circumstances and those of their customers enabling effective ML/FT/PF risk management, including where there are higher risks. Where there are higher risks, the controls implemented under Parts 3 to 9 of the Code should be stronger, more numerous, wider in scope, more frequent or a combination of these. In respect of CDD, the Code specifies particular enhanced measures at paragraphs 14 and 15. On the other hand, where ML/FT/PF risk is lower, each of the requirements must be applied, but they may be applied more narrowly, less frequently or in a reduced way. In respect of CDD, the Code provides for specific exemptions and simplified measures as well as allowing flexibility in how CDD measures are applied where the ML/FT/PF risks are lower, provided the relevant person is able to manage and mitigate those risks.

2.2.4 Risk assessment methodology

Risk assessments should consist of two distinct but related steps:

1. identifying ML/FT/PF risks; and
2. assessing those risks.

2.2.4.1 Identifying ML/FT/PF risks – information sources and relevant risk factors

Code 5(3), 6(3), 7(3)

When identifying ML/FT/PF risks (which simply means finding and listing ML/FT/PF risks) relevant persons must gather sufficient information using a variety of information sources to be satisfied that they have identified and considered all relevant risk factors. The risk factors listed in the Code and the additional risk factors listed in guidance in respect of each type of risk assessment are not exhaustive. Beyond those specified in the Code, relevant persons should determine the risk factors relevant to their/their customers' particular circumstances. However, there is no expectation that relevant persons should deal with all their relevant risk factors to the same extent.

2.2.4.1.1 Information sources

Relevant persons should consider quantitative and qualitative information obtained from relevant internal and external sources determining the type and number of sources to use on a risk sensitive basis. Relevant persons should not normally rely on only one source to identify ML/FT/PF risks.

Relevant persons must have regard to particular sources of information specified in the Code:

Code 5(3), 6(3), 7(3), 15
Code 3(1), 15(5)(a)

- ~~the~~The most recent NRA when conducting the BRA (though it also contains relevant information for CRA and TRAs);
- the BRA when conducting the CRA and TRAs and vice versa;
- ~~List A~~List A specifying jurisdictions against which the FATF has called for countermeasures;

Code 3(1), 15(7)
- ~~List B~~List B specifying jurisdictions with strategic AML/CFT deficiencies and those jurisdictions that may be considered to pose a higher ML/FT risk;

Code 15(5)(b)
- warnings in relation to AML/CFT/CPF matters issued by a competent authority on the Isle of Man;

Code 3(1), 4(1), 13(1), 39(3)
- sanctions lists published by HM Treasury, which have effect in the Island.

In addition, relevant persons should consider:

- information issued by the Island's competent authorities including:
  - policy statements and strategies;
  - guidance;
  - feedback arising from supervisory inspections or other thematic work such as sector reports;
  - alerts;
  - threat reports;
  - typologies;
  - crime statistics;
  - rationales/judgements from actions taken; and
  - ~~List C~~List C specifying jurisdictions which are considered to have an AML/CFT regime of equivalent standard to that of the Isle of Man in relation to key areas of the FATF Recommendations;
- independent audit reports;

Code 8 - 15
- information obtained as part of the relevant person's CDD process and ongoing monitoring of CDD/ECDD (see section 3.4.6) (this is the essential starting point for individual CRAs, but this information is also relevant to the BRA and potentially the TRA); and

Code 13, 33
- relevant transaction records and ongoing monitoring of transactions/activities.

Other sources of information relevant persons should consider on a risk sensitive basis include:

- national risk assessments of the other jurisdiction(s) in which the relevant person operates or customers of a relevant person are located (the European Commission's Supra National Risk Assessment may also be relevant);
- information from industry bodies such as typologies and emerging risks;
- information from civil society, such as corruption indices and country reports;
- information from international standard setting bodies, such as mutual evaluation and follow-up reports, thematic reviews or designations of high risk jurisdictions or legally non-binding black lists;

- information from international institutions and standard setting bodies relevant to ML/FT risks (e.g. UN, IMF, Basel, FATF);
- information from FATF-style regional bodies, such as MONEYVAL, for example mutual evaluation and follow-up reports of jurisdictions and typologies on ML/FT trends, methods and techniques;
- information from credible and reliable open sources such as reports in reputable newspapers;
  information from credible and reliable commercial organisations such as risk and intelligence reports;
- information from statistical organisations and academia;
- the relevant person's own knowledge and professional expertise including information obtained from heads of business and relationship managers or internal audit reports.

2.2.4.1.2 Relevant risk factors

Code 5(3), 6(3), 7(3), 15(5), 15(7)

The Code lists relevant risk factors that relevant persons must have regard to when undertaking their BRA, CRA and TRAs. These lists are not exhaustive or limited, and relevant persons may need to consider other risk factors as appropriate depending on their/their customers' respective circumstances. Consideration should also be given to how certain risk factors may interplay and have an amplifying effect.

Relevant persons must be vigilant when considering risk factors, some of which may indicate suspicious activity.

There is no expectation that relevant persons should deal with all their relevant risk factors to the same extent for every business relationship/occasional transaction. Relevant persons should determine how far it is necessary to deal with a particular risk factor according to their/their customer's respective circumstances.

Guidance on the relevant risk factors listed for each type of risk assessment is found at sections 2.2.8.3, 2.2.9.2, and 2.2.11.2. Relevant persons should note that the risk factors listed relative to each type of risk assessment may be relevant to other risk assessment types.

In addition, the ~~IOMCE~~IOMCI ~~has issued various documents including guidance on financial sanctions, terrorism, terrorist financing, proliferation and proliferation financing.~~
has issued guidance on financial sanctions, terrorism, terrorist financing, proliferation and proliferation financing. Of particular note is a guidance document titled Proliferation Financing Risks, May 2024 which highlights potential proliferation financing specific risk factors, higher risk indicators and red flags.
~~Of particular note is Proliferation Financing Risks, August 2023. This document highlights potential risks to businesses in the Island from proliferation and proliferation financing. It includes guidance on risk assessments in the context of proliferation financing including risk factors, higher risk indicators and red flags.~~

2.2.4.2 Assessing the identified ML/FT/PF risks – risk weighting and classifications

Code 5(1), 6(1), 7(1)

The ML/FT/PF risks identified in the first stage of the process using the relevant risk factors and sources of information must be assessed to determine how these risks affect the relevant person.

This will involve analysing the information obtained to understand the likelihood of the risks occurring and the impact they would have if they did occur. Each type of risk assessment must estimate the ML/FT/PF risk posed in their respective areas. In doing this, relevant persons should take a holistic view of the ML/FT/PF risks they have identified that together will determine the level of ML/FT/PF risk associated with an area of their business or their business as a whole, a particular business relationship/occasional transaction or technology/delivery channel.

Except where paragraph 15(5) of the Code applies, isolated risk factors do not necessarily move a relationship into a higher (or lower) risk category; though relevant persons should note that they could, depending on the particular circumstances.

2.2.4.2.1 Weighting risk factors

When assessing ML/FT/PF risk, relevant persons may decide to weight risk factors differently depending on their relative importance. When weighting risk factors, relevant persons should make an informed judgement about the relevance of different risk factors in the context of their business, the business relationship/occasional transaction or technology, mitigating factors and how the risk factors may affect each other. For example, a relevant person may decide that a customer's personal links to a ~~List B~~List B jurisdiction are less relevant in light of the features of the product they seek. The weight given to each of these risk factors is likely to vary from product to product, customer to customer (or category of customer) and from one relevant person to another. When weighting risk factors relevant persons should ensure that:

- weighting is not unduly influenced by just one factor;
- economic or profit considerations do not influence the risk rating;
- weighting does not lead to a situation where it is impossible for any business relationship etc. to be classified as higher risk;
- situations identified by paragraph 15(5) as matters that pose a higher ML/FT/PF risk cannot be over-ruled by the relevant person's risk weighting; and
- they are able to override any automatically generated risk scores where necessary. The rationale for the decision to override such scores should be documented appropriately.

Code 15(5)

Where a relevant person uses automated IT systems to allocate overall risk scores to categorise business relationships/occasional transactions, it should ensure that:

- it fully understands the risk rating methodology and how it combines, or weights, risk factors to achieve an overall risk score;

- the risk rating methodology used meets the relevant person's risk assessment requirements and their obligations under the Code;
- it is always able to satisfy itself that the scores allocated are accurate and reflect the relevant person's understanding of ML/FT/PF risk;
- it can demonstrate this; and
- there is a mechanism in place to allow a human to examine and override the allocated risk score if necessary.

This may be more relevant where such automated IT systems are not developed in house but purchased from an external provider. Though relevant persons should be aware that even where IT systems are developed in house, over reliance on IT presents potential weaknesses.

Guidance on the TRA covers this in more detail at section 2.2.11.

2.2.4.2.2 Risk classifications

Code 5(1), 6(1), 7(1), 15(4)

The objective of the risk assessments is to estimate the risk of ML/FT/PF posed by the relevant person's business, its customer(s) and relevant technology. Relevant persons should decide on the most appropriate way to estimate ML/FT/PF risk which will depend on the nature and size of the relevant person's business and the types and extent of ML/FT/PF risks to which it is exposed. When estimating the risks, relevant persons may find it helpful to use risk classifications. Classifications for ML/FT/PF risk may assist in understanding the risks (including relative to each other), prioritising and communicating the risks as well as allocating resources to mitigate those risks. They also enable relevant persons to determine whether the use of Code concessions is allowed in any particular case.

Assessing ML/FT/PF risk goes beyond collecting quantitative and qualitative information. It forms the basis for effective and proportionate risk mitigation and should be kept up-to-date to remain relevant.

Code 4(2)(a), 8(3), (4), 9(5), 11(3), (6), 13(1), (4), 14, 15, 16(3), 17(2), (3), 18(3), 19(4), 20(7), 21(4), 22(3), (4)

The Code itself contains two very broad risk classifications particular to CDD procedures and controls. These are "higher risk" (where enhanced CDD requirements apply and specified Code concessions cannot be used) and "not higher risk" (which is everything else, and subject to specified conditions, certain concessions are allowed). The Code does not refer to "low" or "lower" risk. However, the Code does allow relevant persons to adopt more refined risk classifications, provided the requirements for enhanced CDD and the conditions for using Code concessions are adhered to and the relevant person is able to manage and mitigate their ML/FT/PF risks.

Examples of risk classifications (though other classifications are possible) are:

- unacceptable risk – where a relevant person is not satisfied that they are able to manage and mitigate the ML/FT/PF risk;

- higher risk – where a relevant person is satisfied that they are able to manage and mitigate the ML/FT/PF risk by adopting appropriately heightened procedures and controls;
- standard risk - where a relevant person is satisfied that they are able to manage and mitigate the ML/FT/PF risk using standard procedures and controls; and
- lower risk – where a relevant person is satisfied that they are able to manage and mitigate the ML/FT/PF risk applying each of the required AML/CFT/CPF measures, but where the degree, frequency or intensity of the procedures and controls applied may be lighter.

Combinations between these different classifications (medium-high, low medium etc.) may be useful where relevant persons consider they will assist their understanding and prioritisation of ML/FT/PF risks.

2.2.4.2.3 De-risking and unacceptable risk

De-risking is where financial institutions terminate or restrict business relationships with clients or categories of clients to avoid, rather than manage, ML/FT/PF risk in line with the risk based approach. There can be many reasons for de-risking, such as concerns about profitability, reputational risk, lower risk appetites, sanctions regimes and other regulatory requirements. De-risking is not exclusively an AML/CFT/CPF issue. However, from an AML/CFT/CPF perspective, it can introduce further ML/FT/PF risk and opacity into the financial system. Terminating business relationships potentially forces entities and persons underground which creates financial exclusion and reduces transparency meaning transactions are less traceable consequently increasing ML/FT/PF risks. This issue is not unique to the Isle of Man and is recognised internationally. Statements and documents issued by the FATF and MONEYVAL which relevant persons may find useful can be found at:

- FATF clarifies risk based approach: case-by-case, not wholesale de-risking~~,~~ - October 2014;
- Drivers for "de-risking" go beyond anti-money laundering/terrorist financing~~,~~ - June 2015;
- FATF takes action to tackle de-risking~~,~~ - October 2015;
- ~~https://www.coe.int/en/web/moneyval/implementation/de-risking~~MONEYVAL - De-risking ~~-,~~ April 2015.

Relevant persons are encouraged to avoid policies that support the wholesale de-risking of business categories without taking into account, seriously and comprehensively, their level of ML/FT/PF risk and applicable risk mitigation measures for customers within a particular sector. Decisions with respect to unacceptable risk customers should be made on a case-by case-basis.

2.2.5 Managing and mitigating ML/FT/PF risks

Code 4(2), 15(4)

Following ML/FT/PF risk assessments, whether at the point of an initial risk assessment or after a review, relevant persons must determine and adopt

appropriate and effective risk sensitive procedures and controls which enable them to manage and mitigate their ML/FT/PF risks. This means that heightened (or in the case of CDD, enhanced) measures should be taken to manage and mitigate situations in which the ML/FT/PF risk is higher, and Code concessions must not be applied. Less stringent measures may be applied in situations with lower ML/FT/PF risk.

Relevant persons should note that where a customer has been assessed as lower risk, this does not necessarily mean that it would be appropriate to apply less stringent measures in respect of all CDD requirements. For example, it may be appropriate to apply less stringent verification measures, but it may still be appropriate to apply a standard level of ongoing monitoring procedures and controls.

Specific guidance on the mitigation procedures and controls required by the Code are provided in relevant sections of this Handbook.

2.2.6 Risk assessment reviews

Code 5(2)(c), 6(2)(c), 7(2)(e)

5 Business risk assessment / 6 Customer risk assessment / 7 Technology risk assessment

(2) business/customer/technology risk assessment must be –

(c)/(e) regularly reviewed (details of any review must be recorded) and, if appropriate, amended so as to keep the assessment/it up-to-date.

Code 4, 5, 6, 7

Relevant persons must establish, record, operate and maintain procedures and controls for conducting risk assessment reviews so as to ensure their risk assessments remain up to date and relevant in every case.

Risk assessments must be reviewed periodically, but in order to ensure the relevant person can manage and mitigate its ML/FT/PF risks, risk assessments should also be reviewed when circumstances change or relevant new threats or technologies emerge.

It is a matter for relevant persons to determine the depth and frequency of their ML/FT/PF risk assessment reviews, though relevant persons should be cognisant of the overarching requirement that their procedures must enable them to manage and mitigate their ML/FT/PF risks. Considerations in determining the depth and frequency of reviews include, but are not limited to, the factors listed below.

- The ML/FT/PF risks as assessed in the initial risk assessments. Any risk classifications applied in the initial risk assessments may assist relevant persons in determining the appropriate depth and frequency of risk assessment reviews.
- Any developments occurring since the initial risk assessments were completed, for example in relation to the relevant person's particular

circumstances and/or the broader environment in which they operate, or in the circumstances of their customers (collectively and/or individually).

- In respect of CRAs, information obtained as part of the ongoing monitoring of a business relationship should be assessed and consideration given as to whether it affects the CRA.

Code 30

Examples of procedures and controls to ensure risk assessments are regularly reviewed and remain relevant include, but are not limited to, the factors listed below.

- Setting a particular date for each calendar year for a periodic BRA/TRA review to take place. Relevant persons should be aware that the first BRA and TRA may need to be reviewed on a shorter time frame than future BRAs and TRAs to assess whether the assumptions made before business commenced reflect the business that is being carried out.
- Setting a date on a risk sensitive basis for CRA reviews to ensure new or emerging risks are included.
- Reflecting new/emerging risks, risks that have increased or changes in circumstances (where appropriate) within the risk assessment(s) as soon as possible.
- Carefully recording issues throughout the year that could have a bearing on risk assessments such as:
    - external and internal suspicious activity reports;
    - compliance failures and intelligence from staff; or
    - findings from monitoring and testing compliance including internal/external audit reports.

To ensure risk assessment reviews are effective, relevant persons should ensure the systems and controls are in place to identify and assess emerging ML/FT/PF risks, in order that these risks can be incorporated into their risk assessments, where appropriate, in a timely manner. Examples of systems and controls to identify emerging risks include, but are not limited to, the factors listed below.

- Processes to ensure that internal information, including from those who interact with customers, information obtained as part of ongoing monitoring of business relationships, compliance risk management and internal audit departments (where relevant), is reviewed regularly to identify trends and emerging issues, in relation to both individual relationships and the relevant person's business including any relevant technologies.

Code 4(1)(a)

- Processes to ensure the relevant person regularly reviews relevant information sources such as those listed above at section 2.2.4.1.1.
    - in respect of BRA/TRAs this should involve regularly reviewing:
        - law enforcement alerts and reports;

- thematic reviews and similar publications issued by competent authorities; and

- processes to capture and review information on risks, in particular risks relating to new categories of customers, countries or geographical areas, new products, new services, new distribution channels and new compliance systems and controls.

  - in respect of CRAs this should involve regularly reviewing:
    - terror alerts and sanctions regimes to ensure the relevant person becomes aware of changes as soon as they are issued or communicated and ensure that these are acted upon as necessary;
    - media reports relevant to the sectors/jurisdictions in which the relevant person is active;

- Engagement with other industry ~~representative~~representatives and competent authorities, and processes to communicate findings to relevant staff.
- Establishing a culture of information sharing and strong ethics within the relevant person.

As with the initial risk assessments, updates to risk assessments and changes to CDD measures and other AML/CFT/CPF procedures and controls as a result of the review process should be proportionate to the ML/FT/PF risk.

2.2.7 Recording risk assessments

Code 5(2), 6(2), 7(2)

5 Business risk assessment / 6 Customer risk assessment / 7 Technology risk assessment

(2) The business/customer/technology risk assessment must be –

(b)/(d) recorded in order to be able to demonstrate its basis;

The robustness, objectivity and reasonableness of both an initial risk assessment and any risk assessment review and their outcomes must be demonstrable and evidenced at all times. All aspects of the risk assessment and any subsequent reviews, or changes made as a result of reviews or monitoring should be documented and recorded with supporting information and documents retained. This should be done in such a way that the relevant person and competent authorities are able to understand how a risk assessment/review was conducted (including any internal sign-off procedures and risk weightings and classifications allocated) and why it was conducted in a particular way.

Code (5)(2), 7(2)

Relevant persons should maintain a detailed version or control history within the risk assessment(s), alongside any supporting documentation and evidence to better demonstrate compliance with the Code.

2.2.8 Business risk assessment ("BRA")

Code 5(1)

5 Business risk assessment
(1) A relevant person must carry out an assessment that estimates the risk of ML/FT posed by the relevant person's business and customers.

The purpose of a BRA is to assist relevant persons to understand where, how and to what extent they are exposed to ML/FT/PF risk and which areas of their business they should prioritise in combatting ML/FT/PF. The BRA should form the basis of a relevant person's risk based approach and its risk appetite making clear the types of risk and the risk level the relevant person is prepared to accept. It is the necessary foundation for determining the nature and extent of AML/CFT/CPF resources and should be used to inform the policies, procedures and controls to mitigate ML/FT/PF risk, including decisions on the appropriate level and type of CDD to be applied in specific situations to particular types of customers, products, services and delivery channels.

The BRA should be considered a living, ever-changing, ongoing document, which utilises recent data, findings and trends from the business and its customers but also documents and describes the current controls, mitigations, risks and threats to, and within, the relevant person's business.

2.2.8.1 Tailored and proportionate

Conducting a BRA requires reasoned judgements and will very much depend on the particular circumstances of the relevant person. The BRA must be tailored to the relevant person's business including where the relevant person is part of a group. Relevant persons may not be able to rely on group wide BRAs to satisfy the Code's BRA requirements. In determining whether it is appropriate to accept a group wide BRA, relevant persons should consider whether it is sufficiently granular and specific to reflect the relevant person's business and their particular ML/FT/PF risks. Relevant persons should also consider whether the group wide BRA reflects the ML/FT/PF risks that the relevant person is exposed to as a result of the group's links to certain geographical areas. If the group's BRA is not adequately specific and/or does not cover the Code's requirements for the relevant person, the relevant person must complement it with their own BRA. In addition, the relevant person's BRA should reflect any connections the group has with jurisdictions associated with high levels of corruption or AML/CFT/CPF deficiencies even if the group's BRA is silent on this point.

The steps relevant persons take to identify and assess ML/FT/PF risk across their business must be proportionate to the size and nature of their business. Where relevant persons do not offer complex products or services and have limited or no international exposure a simple BRA may be sufficient; where a simple BRA is utilised, the BRA must still as a minimum have adequate regard to all of the risk factors detailed in paragraph 5(3) of the Code. Whereas, relevant persons offering

more complex products and services, and/or where there are multiple subsidiaries/branches offering a wide variety of products, and/or the relevant person's customer base is more diverse, a more sophisticated BRA will be required. No two BRAs will be the same, however all BRAs must document and evidence that the relevant person has carried out an assessment that estimates the risk of ML/FT/PF posed by the relevant person's business and customers.

2.2.8.2 Timing of the BRA

Code 5(2)

5 Business risk assessment

(2) The business risk assessment must be –

(a) undertaken as soon as reasonably practicable after the relevant person commences business;

Code 4(1)

All existing relevant persons must already have undertaken a BRA. This must be documented and recorded in line with paragraph 4 of the Code. Newly licensed or registered relevant persons must undertake the BRA before entering into or carrying on a business relationship/occasional transaction.

2.2.8.3 Relevant risk factors

Code 5(3)

5 Business risk assessment

(3) The business risk assessment must have regard to all relevant risk factors, including –

(a) the nature, scale and complexity of the relevant person's activities;

(b) any relevant findings of the most recent National Risk Assessment relating to the Island;

(c) the products and services provided by the relevant person;

(d) the manner in which the products and services are provided, including whether the relevant person meets its customers;

(e) the involvement of any third parties for elements of the customer due diligence process, including where reliance is placed on a third party;

(f) customer risk assessments carried out under paragraph 6; and

(g) any technology risk assessment carried out under paragraph 7.

Guidance regarding the relevant risk factors listed at paragraph 5(3) of the Code is supplemented by other risk factors that may be applicable to relevant persons.

In addition, the ~~IOMCE~~IOMCI has issued guidance on financial sanctions, terrorism, ~~terrorist financing,~~terrorist financing, proliferation and ~~proliferation financing.~~proliferation financing. Of particular note is a guidance document titled ~~Proliferation Financing Risks, August 2023~~ Proliferation Financing Risks, May 2024 which highlights potential proliferation financing specific risk factors, higher risk indicators and red flags.

These lists are not exhaustive or limited, nor is there an expectation that relevant persons should deal with all their relevant risk factors to the same extent in all cases.

Code 5(3)(a)

The nature, scale and complexity of the relevant person's activities

Relevant persons should consider the risks related to:

- structural factors outside the relevant person such as:
  - whether the relevant person is a standalone operation or operates within a group structure;
  - the role of the relevant person within any group structure;
  - any influence on the relevant person or support that may come from the group structure;
  - any influence on the relevant person or support that may come from third parties outside the relevant person/group structure.
- structural factors within the relevant person such as:
  - management structures and levels of sign off authorities;
  - high concentrations of roles and responsibilities (for example, an employee with responsibility for so many AML/CFT/CPF procedures and controls such that if there were an issue, it would be easy for them to conceal and/or if not carried out competently would be difficult for others in the relevant person or management to spot as fewer people involved in stages or elements of AML/CFT/CPF work);
  - diluted roles and responsibilities (for example, employees having so small a part in the AML/CFT/CPF procedures and controls such that no one employee can view the overall position meaning that abuse of the relationship is difficult to identify);
  - the level of compliance resources available.

Code 5(3)(e), 6(3)(e), 7(3)

- organisational factors such as outsourcing aspects of regulated activities, AML/CFT/CPF or other compliance functions. Guidance on outsourcing as a relevant risk factor can be found below in respect of Code paragraphs 5(3)(e) and 6(3)(e) and 7(3);
- the diversity of its operations and implications of this diversity, such as the degree of risk associated with each area of its operation or the relevant person's ability to understand and mitigate the risks of each area;
- the volume and size of each area of operation;
- concentrations of business in any particular area such as customers, jurisdictions, products or services;
- the volume and size of its transactions;
- the services provided by the business and how those services might be abused for ML/FT/PF; and
- the scale on which products and services are provided.

Code 5(3)(f), 6(3)(b)

Geographic and country risk

Though the Code does not explicitly refer to geographic risk as a BRA relevant risk factor (except through the CRA) depending on the circumstances of the relevant person, geographic risk (whether this concerns a particular country, geographic area or border region within a country), can be relevant to the BRA. A relevant person should have regard to the jurisdictions they are exposed to whether through their own activities and operations, those of other group entities, the activities of its customers or its customers' beneficial owners/beneficiaries or through any third parties on whom reliance is placed. This includes jurisdictions where relevant persons / group entities / customers / beneficial owners / beneficiaries / third parties etc.:

- are based;
- have main places of business; or
- have any personal links with a jurisdiction of which the relevant person should reasonably be aware.

Relevant persons should also consider any vulnerabilities within the relevant person (or the wider organisation) in the jurisdiction(s).

This guidance on geographic risk in the context of BRAs is supplemented with guidance on geographic risk at section 2.2.9 in respect of CRAs.

Code 5(3)(b)

Any relevant findings of the most recent National Risk Assessment relating to the Island

The Isle of Man Government's latest NRA and related documents and information can be found here~~.~~, as at the time of publication this assessment is being revised. Regulated entities are obliged to undertake and update their BRA and this must have regard to any relevant findings of the most recent NRA relating to the Island.

Relevant persons should include assessment and analysis of any identified findings, trends, vulnerabilities and risks associated with each relevant persons' sector(s) from the Island's latest NRA. ~~When identifying findings or trends,~~Industry must be able to show how they have considered and mitigated the relevant ~~person should consider the impact these~~risks and vulnerabilities ~~have on their business and the mitigation in place.~~ identified.

There are a number of risk assessments, including sectoral and topical NRAs, that form part of the Island's NRA which will be published over the course 2025. It is encouraged that each NRA is considered as it is published, however the relevant person may update their overall BRA at its next formal review date. Firms must include consideration for all topical NRAs and any relevant sectoral NRAs within the firms BRA. This should be done by January 2026.

Isle of Man National Risk Assessment

Topical Risk Assessments	Sectoral Risk Assessments[2]
Terrorist Financing	Accountants & Tax Advisers
Proliferation Financing	Advocates & Registered Legal Persons
Money Laundering	Estate Agents
Cross Border & National Threats[3]	High Value Goods Dealers
Legal Persons & Arrangements	Money Lenders
Risk Appetite Statement[4]	Non-Profit Organisations
The Isle of Man Profile[5]	Payroll
	Safe Custody
	Virtual Assets & Virtual Asset Service Providers
	Banking
	Crowdfunding[6]
	Financial Advisory
	Funds (Services to Collective Investment Schemes)
	Investment Business
	Money Transmission Services
	Trust & Corporate Service Providers
	Insurance (Life)
	Non-Life Insurance
	Pensions
	Gambling

Code 5(3)(c)

The products and services provided by the relevant person and associated transactions

Though not specifically listed in the Code, this section also covers transactions associated with products and services provided by relevant persons.

Code 15(7)(h)

The Code notes that the provision of high-risk products may pose a higher ML/FT/PF risk. When identifying and assessing the ML/FT/PF risk associated with their products, services and transactions, relevant persons should consider the risks related to:

- The level of transparency, or opaqueness of the products, services or transactions, relevant risk factors include, but are not limited to, those listed below.
    - The extent to which products or services facilitate, or allow anonymity or opaqueness of customers, beneficial owners or beneficiary structures to facilitate hiding their identity such that they could potentially be used for illicit purposes. For example pooled accounts, bearer shares, fiduciary deposits,

[2] Some sectoral assessments will be published as standalone assessment and others will be incorporated into the Money Laundering NRA,
[3] Not in the public domain
[4] Not a formal NRA but should be considered as part of the review of NRAs.
[5] Not a formal NRA but should be considered as part of the review of NRAs.
[6] To be delayed as no entities operating at this time

certain trusts, legal entities structured in a way to take advantage of anonymity, dealings with shell companies or companies with nominee shareholders.
    - The extent to which it is possible for a third party that is not part of the business relationship to give instructions, for example, certain correspondent banking relationships;
    - The complexity of the products, services and transactions, relevant risk factors include: the extent that the transaction is complex and involves multiple parties or multiple jurisdictions e.g. certain trade finance transactions;
    - conversely, the extent that the transaction is straightforward e.g. regular payments into a pension fund;
    - the extent that the products or services allow payments from third parties or accept overpayments; where third party payments are permitted, the extent to which:
        - the relevant person can identify the third party and understands their relationship with the customer, for example a state welfare body or a guarantor; and
        - products and services are funded primarily by fund transfers from the customer's own account at another financial institution that is subject to AML/CFT/CPF standards and oversight comparable to those required under the Code; and
    - the risks associated with new or innovative products and services, in particular where this involves the use of new technologies or payment methods.

Code 15

- the value or size of the products, services or transactions, relevant risk factors include:
    - the provision of services to high-net worth individuals; relevant persons should note that even seemingly standard transactions might be higher risk if used by potentially higher risk customers.
    - the extent that products or services may be cash intensive e.g. certain types of payment services and current accounts.
    - the extent that products or services facilitate or encourage high value transactions e.g. there are no caps on certain transaction values or levels of premium that could limit the use of the product or services for ML/FT/PF purposes.

Code 5(3)(d), 6(3)(c), (g), (e)

The manner in which the products and services are provided, including whether the relevant person meets its customers

Considerations particular to the manner in which products and services are provided to customers, including whether the relevant person meets its customers can be found at section 2.2.9.2 in the CRA guidance, particularly with respect to Code sub-paragraphs:

- 6(3)(c) on the manner in which products and services are provided;

- 6(3)(g) on whether the relevant person and the customer have met;
- 6(3)(e) on the involvement of third parties.

CRA guidance in this area should be considered (with any necessary alterations to make it relevant to the specific requirements of BRAs) as part of the BRA.

Code 7|(2)(d)

In addition, the way technology is used to deliver products and services is considered in respect of Code sub-paragraph 7(2)(d) (the TRA is discussed in section 2.2.11). These considerations should be reflected in the BRA.

Code 5(3)(e), 9, 12(2)(b) 17, 19, 21, 22

The Code specifies a number of ways third parties can be involved in elements of the CDD process, namely introduced business, eligibly introduced business, persons in the regulated sector acting on behalf of a third party, certain miscellaneous concessions where the relevant person is not required to comply with paragraph 12(2)(b) and transfers of blocks of business.

Outsourcing is also an area where third parties can be involved in elements of the CDD process. When identifying and assessing the ML/FT/PF risk associated with outsourcing elements of the CDD process, consideration should include:

- the quality of control mechanisms in place such as clarity of the division of roles and responsibilities and the quality of management information and reporting;
- whether the provider is a trusted person;
- reputational issues concerning the provider;
- previous experiences with the provider;
- outsourcing of processes or functions by the provider and the potential for and impact of chains of outsourcing; and
- quality of assurance mechanisms and the results of any audits or inspections where the material generated as a result of outsourcing to the provider has been reviewed.

The European Banking Authority has issued Guidelines on Outsourcing Arrangements which all categories of relevant persons may find useful when considering the risks associated with outsourcing elements of the CDD process.

Relevant persons should also ensure adherence to regulatory requirements and guidance in respect of any outsourcing or delegations entered into.

Code 5(3)(e), 9, 12(2)(b) 17, 19, 21, 22

The involvement of any third parties for elements of the CDD process, including where reliance is placed on a third party

The Code specifies a number of ways third parties can be involved in elements of the CDD process, namely introduced business, eligibly introduced business, persons in the regulated sector acting on behalf of a third party, certain miscellaneous concessions where the relevant person is not required to comply with paragraph 12(2)(b) and transfers of blocks of business.

Outsourcing is also an area where third parties can be involved in elements of the CDD process. When identifying and assessing the ML/FT/PF risk associated with outsourcing elements of the CDD process, consideration should include:

- the quality of control mechanisms in place such as clarity of the division of roles and responsibilities and the quality of management information and reporting;
- whether the provider is a trusted person;
- reputational issues concerning the provider;
- previous experiences with the provider;
- outsourcing of processes or functions by the provider and the potential for and impact of chains of outsourcing; and
- quality of assurance mechanisms and the results of any audits or inspections where the material generated as a result of outsourcing to the provider has been reviewed.

The European Banking Authority has issued Guidelines on Outsourcing Arrangements which all categories of relevant persons may find useful when considering the risks associated with outsourcing elements of the CDD process.

Relevant persons should also ensure adherence to regulatory requirements and guidance in respect of any outsourcing or delegations entered into.

The guidance at section 2.2.9.2 on CRAs regarding the risks when third parties are involved or relied on in the CDD process may be used by relevant persons to assist in dealing with this requirement subject to appropriate amendments.

Code 5(3)(f), 6

Customer risk assessments carried out under paragraph 6 of the Code

CRAs must be considered as part of the BRA. The BRA and the CRAs are in a continuous feedback loop, with the BRA informing each of the CRAs and the CRAs informing the BRA.

The BRA should make reference to the relevant person's customer base, particularly highlighting higher risk relationships and the proportion of the customer base such customers represent. The statistical data, outcomes, trends and findings from the CRAs carried out should be considered, documented and assessed within the relevant person's BRA.

Code 5(3)(g), 7

Any technology risk assessment carried out under paragraph 7 of the Code

The TRA undertaken by the relevant person must be considered as part of the BRA. The BRA should make reference to the TRA, and consider the TRA's ML/FT/PF risk outcomes and findings.

2.2.9 Customer risk assessment ("CRA")

Code 6(1)

6 Customer risk assessment

(1) A relevant person must carry out an assessment that estimates the risk of ML/FT/PF posed by the relevant person's customer.

A documented customer risk assessment is required for every customer, regardless of when the business relationship was established. Similarly, the regular reviews of CRA required by the Code also need to be recorded.

Code 6(3)

The purpose of conducting a risk assessment for each of a relevant person's customers is to assist relevant persons to understand how a particular customer exposes them to ML/FT/PF risk and enable them to apply their procedures appropriately to that customer in order to effectively mitigate the ML/FT/PF risk that customer poses. Relevant persons should seek to obtain a holistic view of the business relationship/occasional transaction. This will require gathering enough information, including enhanced CDD where appropriate, to be satisfied that they have identified all relevant risk factors (including those listed in the Code) for assessment and mitigation. It is prudent for relevant persons to start from a position of higher risk and mitigate risk factors accordingly as the CRA is undertaken.

Relevant persons should note that there is no expectation to consider all the additional risk factors listed in this guidance in all cases, and not all relevant risk factors will need to be considered to the same extent for every business relationship/occasional transaction. Relevant persons should determine how far it is necessary to deal with a particular risk factor according to their/their customer's respective circumstances. In addition, the risk factors listed in the Code and guidance are not exhaustive. What risk factors (beyond those listed in the Code) are relevant with respect to any particular business relationship/occasional transaction is a matter for relevant persons to decide on a case-by-case basis.

Relevant persons should note that assessing a customer as higher ML/FT/PF risk does not automatically mean a customer is a money launderer or is financing terrorism. Similarly, assessing a customer as low ML/FT/PF risk does not mean the customer presents no risk at all. In addition, there is no regulatory impediment to relevant persons having higher risk customers, provided the relevant person's procedures and controls enable them to demonstrably manage and mitigate the ML/FT/PF risk and the relevant person complies with the enhanced CDD requirements and restrictions on exemptions and simplified measures within the Code.

2.2.9.1 Timing of the CRA

Code 6(2)(a)

6 Customer risk assessment

(2) A customer risk assessment must be –

(a) undertaken prior to the establishment of a business relationship or the carrying out of an occasional transaction with or for that customer;

Unlike with verification of identity requirements, there is no timing concession for CRAs[7], which must be undertaken before a business relationship is established or an occasional transaction undertaken for that customer.

CRAs and CDD measures are in a continuous feedback loop. The initial CDD obtained on a customer allows relevant persons to undertake an initial CRA of that business relationship/occasional transaction. This initial CRA enables the relevant person to determine whether the initial CDD obtained is sufficient for that business relationship/occasional transaction. The extent of CDD ultimately obtained, whether the use of enhanced or simplified measures are appropriate, and the extent of ongoing monitoring is dependent on the findings of the CRA. Consequently, the CRA must be viewed as a living document that develops as more documents, data and information is obtained for that customer.

2.2.9.2 Relevant risk factors including matters that pose or may pose higher ML/FT/PF risks

Code 6(3), 5, 15(5), (7), 9(4)

6 Customer risk assessment

(3) The customer risk assessment must have regard to all relevant risk factors, including –

(a) the business risk assessment carried out under paragraph 5;

(b) the nature, scale, complexity and location of the customer's activities;

(c) the manner in which the products and services are provided to the customer;

(d) the risk factors included in paragraph 15(5) and (7);

(e) the involvement of any third parties for elements of the customer due diligence process, including where reliance is placed on a third party;

(f) any risk assessment carried out under paragraph 9(4); and

(g) whether the relevant person and the customer have met during the business relationship, or its formation, or in the course of an occasional transaction.

Code 15(5)

15 Enhanced customer due diligence

(5) Matters that pose a higher risk of ML/FT include –

(a) a business relationship or occasional transaction with a customer that is resident or located in a jurisdiction in List A; and

(b) a customer that is the subject of a warning in relation to AML/CFT matters issued by a competent authority or equivalent authority in another jurisdiction.

Code 15(7)

15 Enhanced customer due diligence

(7) matters that may pose a higher risk of ML/FT include –

[7] CRAs are sometimes referred to as "customer risk profiles".

(a) activity in a jurisdiction the relevant person deems to be higher risk of ML/FT;

(b) a business relationship or occasional transaction with a customer resident or located in a jurisdiction in List B;

(c) activity in a jurisdiction in List A or B;

(d) a situation that by its nature presents an increased risk of ML/FT;

(e) a business relationship or occasional transaction with a PEP;

(f) a company that has nominee shareholders or shares in bearer form;

(g) the provision of high risk products;

(h) the provision of services to high-net-worth individuals;

(i) a legal arrangement;

(j) persons performing prominent functions for international organisations;

(k) circumstances in which the relevant persons and the customer have not met –

(i) during the business relationship or during its formation; or

(ii) in the course of an occasional transaction; and

(l) if the beneficiary of a life insurance policy is a legal person or legal arrangement.

The need for relevant persons to gather sufficient information to be satisfied they have identified all relevant risk factors will, in the context of CRAs, include applying additional CDD measures where necessary. Relevant persons should assess those risk factors to obtain a holistic view of the risk associated with a particular business relationship/occasional transaction.

The matters stipulated by the Code as posing a higher ML/FT/PF risk, are incorporated into the relevant risk factors listed below.

The matters outlined by the Code that may pose a higher risk are dealt with throughout the BRA, CRA and PEP guidance.

~~In addition, the IOMCE has issued guidance on financial sanctions, terrorism, terrorist financing, proliferation and proliferation financing. Of particular note is Proliferation Financing Risks, August 2023) which highlights potential proliferation financing specific risk factors, higher risk indicators and red flags.~~

Code 6(3)(a)

The business risk assessment carried out under paragraph 5

The findings of the BRA, including the NRA should inform each CRA. The BRA and the CRAs are in a continuous feedback loop, with the BRA informing each of the CRAs and the CRAs informing the BRA.

Code 6(3)(b)

The nature, scale, complexity and location of the customer's (including the customer's beneficial owner's) activities

Nature, scale and complexity

The Code notes a number of matters relevant to a customer's/beneficial owner's activities that may pose a higher ML/FT/PF risk. When identifying and assessing the ML/FT/PF risks regarding a customer's/beneficial owner's activities, considerations should include whether the customer or its beneficial owner(s):

Code 15(7)(e)

- has political connections, such as:
  - the customer or its beneficial owner is a Politically Exposed Person ("PEP") or has any other relevant links to a PEP; or
  - one or more of the customer's directors (or equivalent) are PEPs and if so, whether these PEPs exercise significant control over the customer or beneficial owner~~;~~.

Code 14

Note that where a customer or its beneficial owner is a PEP, paragraph 14 of the Code applies. Further guidance on PEPs can be found at section 3.8.8.

- performs prominent functions for international organisations, including considering having commercial connections ("a CEP[8]") to higher risk occupational activities that are commonly associated with higher corruption risk, such as:

Code 15(7)(g), (j)

  - Arms / weapons trading, dealing and defence;
  - Casinos, gambling and betting;
  - Construction / development industry;
  - Dating / adult entertainment industry;
  - Decision-making members of high profile sporting bodies;
  - Import/export companies/industry;
  - Money services businesses;
  - Oil and gas industry;
  - Pharmaceuticals and healthcare;
  - Precious metals and stones mining and trading;
  - Shipping and transport of goods; and
  - Virtual asset service providers.

[8] A commercially exposed person ("CEP") is an individual who is associated with a specific industry activity which typically has a higher exposure to bribery and corruption, which, in turn, may increase the ML/FT/PF/PF risk posed to the firm by such individuals where they are affiliated to a customer. An individual would be regarded as a CEP due to their position as a senior executive of a commercial enterprise in an industry posing a higher risk of financial crime. For example; a Board member, senior executive, or person with decision-making power or influence in one of the listed occupational activities would be considered a CEP. However, an administrator or employee with no decision-making power or influence would not be classed as a CEP.

- Is a CEP that holds prominent position or enjoys a high public profile that might enable them to abuse this position for private gain; for example, they are:
    - persons performing prominent functions for international organisations;
    - senior local or regional public officials with the ability to influence the awarding of public contracts;
    - decision-making members of high profile sporting bodies;
    - individuals that are known to influence the government and other senior decision-makers.

- has links to sectors that involve significant amounts of cash;
- is dealing with complex equipment etc. for which he/she/it lacks technical background or which is incongruent with their stated activities;
- engages in complex trade deals involving third parties in lines of business that do not accord with their stated business activities established at on-boarding;
- though declared to be a commercial business, conducts transactions that suggest they are acting as a money remittance business or a pay through account i.e. accounts involving a rapid movement of high volume transactions with a small end of day balance without clear business rationale;
- engages in or request payments be made to third parties or third party destinations that do not accord with the customer's stated business activities and/or where they are not party to the underlying transaction(s) being paid for;
- is affiliated with a university or research institution involved in the trading of potentially proliferation sensitive or export controlled items;

Code 15(7)(f), (i), (l)

- is a legal person or a legal arrangement and if so, the purpose of their establishment and the nature of their business. Or if the matter involves the beneficiary of a life insurance policy, whether that beneficiary is a legal person or legal arrangement;
- is a legal person with nominee shareholders or shares in bearer form;
- is a legal person subject to enforceable disclosure requirements that ensure that reliable information about the customer's beneficial owner is publicly available, for example public companies listed on stock exchanges that make disclosure a listing condition;
- is a public or state owned entity and if so whether it is from a jurisdiction with low or high levels of corruption;

Code 16(3)

- is an acceptable applicant in accordance with paragraph 16(3) of the Code;
- is subject to supervisory or enforcement action for failure to comply with AML/CFT/CPF obligations or wider conduct requirements in recent years; and

- background is consistent with what the relevant persons knows about it, for example:
    - its former, current or planned business activity;
    - the turnover of the business;
    - its source of funds; and
    - the customer's or beneficial owner's source of wealth.
    -

Code 6(3)(b)

Location of the customer's activities - Geographic risk

Though it is not reiterated here, the BRA guidance on geographic risk may be relevant when undertaking CRAs.

Code 15(5)

Where a business relationship/occasional transaction is with a customer resident or located in a jurisdiction in List AList A, the Code requires that business relationship/occasional transaction to be deemed higher risk and subject to enhanced CDD.

Code 15(7)

The Code specifies other geographic risk situations that may pose a higher ML/FT/PF risk. These are activity in a List A or B jurisdiction or a jurisdiction the relevant person has deemed to be higher ML/FT/PF risk, or residency in a List B jurisdiction. When assessing whether to deem a jurisdiction higher risk or whether these matters do pose a higher risk in respect of any particular case, relevant persons should consider the factors listed below.

- **The nature and purpose of the business relationship/occasional transaction within the jurisdiction(s)**.
  This will often determine the relative importance of individual geographic risk factors, and consequently the weighting given to them in the assessment. Considerations should include, for example:
    - where funds used in the business relationship/occasional transaction are/were generated abroad, the level of predicate offences relevant to ML and the effectiveness of the jurisdiction's legal system;
    - where funds are received from or sent to jurisdictions where groups committing terrorist offences are known to be operating, the extent to which this is expected or might give rise to suspicion based on what the relevant person knows about the nature and purpose of the business relationship/occasional transaction;
    - whether the customer (or its beneficial owner(s) engage in or request payments be made to third parties or third party destinations that do not accord with their stated business activities and/or where they are not party to the underlying transaction(s) being paid for;
    - where the customer is a business which is equivalent to business in the regulated sector as set out in Schedule 4 to POCA, the adequacy of the country's AML/CFT/CPF regime and the effectiveness of AML/CFT/CPF supervision; or

- where the customer is not a natural person, the extent to which the country in which the customer (and where applicable, the beneficial owner(s)/controller(s)) is registered, effectively complies with international tax transparency standards.

- **The level of predicate offences relevant to money laundering within the jurisdiction.**
  Considerations should include, for example:
  - levels of organised crime, corruption, tax crime or serious fraud or other criminal activity, including as source or transit countries for illegal drugs, human trafficking and smuggling and illegal gambling based on information from credible and reliable public sources. Examples of possible sources include:
    - corruption perception indices;
    - OECD country reports on the implementation of the OECD's anti-bribery convention; and
    - the United Nations Office on Drugs and Crime World Drug Report.
  - the capacity of the jurisdiction's investigative and judicial system to investigate and prosecute these offences effectively based on information from more than one credible and reliable source.

- **The level of FT ~~(including FP)~~ risk within a jurisdiction~~.~~.**
  Considerations should include, for example:
  - whether the jurisdiction is identified as providing funding or support for terrorist activities or has designated terrorist organisations operating within it, according to law enforcement or credible and reliable open media sources; and
  - any economic or financial sanctions, embargoes or similar measures issued against a jurisdiction, by for example the UN.
    - The Authority has issued a TF Factsheet for information on TF.

- **The level of PF risk within a jurisdiction.**
  Considerations should include, for example:
  - whether the jurisdiction is identified as a country of proliferation or diversion concern; and
  - any economic or financial sanctions, embargoes or similar measures issued against a jurisdiction, by for example the UN.
    - The Authority has issued a PF Factsheet for information on PF.

Code 3(1), 15(5), (7)

- **The effectiveness of the jurisdiction's AML/CFT/CPF regime including the strength of its governance, law enforcement, and regulatory/supervisory regimes.**

  Considerations should include, for example:
  - ~~whether the jurisdiction is present on List A or List B;~~
  - whether the jurisdiction is present on List A or List B;
  - there is information from one or more credible and reliable sources about the quality of the jurisdiction's AML/CFT controls, including information about the quality and effectiveness of regulatory enforcement and oversight. Examples of possible sources include:
    - FATF or FATF-Style Regional Body ("FSRB") mutual evaluation reports (the executive summary and key findings as well as the assessment of compliance with FATF Recommendations 10, 26 and 27 and Immediate Outcomes 3 and 4 are particularly useful~~).~~. Relevant persons should be aware that membership of the FATF or an FSRB does not, of itself, mean that the jurisdiction's AML/CFT regime is adequate and effective;
    - International Monetary Fund country assessments; and
    - World Bank and International Monetary Fund Financial Sector Assessment Program reports.

Code 3(1) Relevant persons may use ~~List C~~List C, which specifies jurisdictions considered to have an AML/CFT regime of equivalent standard to the Isle of Man in relation to key areas of the FATF Recommendations, to identify jurisdictions that may present a lower risk.

- **The level of legal and beneficial ownership transparency and tax compliance within the jurisdiction.**
  Considerations should include, for example, whether:
  - the country has been deemed compliant with international tax transparency and information sharing standards and there is evidence that relevant rules are effectively implemented in practice according to information from more than one credible and reliable source. Examples of possible sources include:
    - reports by the OECD's Global Forum on Transparency and the Exchange of Information for Tax Purposes, which rate jurisdictions for tax transparency and information sharing purposes;
    - assessments of the jurisdiction's commitment to automatic exchange of information based on the Common Reporting Standard;

        - assessments by the FATF or FSRBs of the jurisdiction's compliance with FATF Recommendations 9, 24 and 25 and Immediate Outcomes 2 and 5; or
        - FSRB or IMF assessments;
    - the jurisdiction is committed to, and has effectively implemented, the Common Reporting Standard on Automatic Exchange of Information, which the G20 adopted in 2014; and
    - the jurisdiction has put in place reliable and accessible beneficial ownership registers.

Code 15(5)(b)

The customer's and the customer's beneficial owner's reputation

A customer's/customer's beneficial owner's reputation is not specifically referred to in the Code, however, paragraph 15(5)(b) stipulates that where a customer is the subject of a warning in relation to AML/CFT/CPF matters issued by a competent authority or equivalent authority in another jurisdiction it must be deemed higher risk and subject to enhanced CDD.

Other risk factors associated with a customer's (including where relevant the customer's senior management) or their beneficial owner's reputation include, for example, whether:

- the customer, beneficial owner or anyone publicly known to be closely associated with them currently, or in the past, has had their assets frozen due to administrative or criminal proceedings e.g. sanctions or allegations of terrorism or financing of terrorism;
- the customer or beneficial owner has been the subject of a suspicious activity report by the relevant person in the past, or the subject to a request for information from a competent authority;
- the relevant person has in-house information about the customer's or their beneficial owner's integrity, obtained, for example, in the course of a long-standing business relationship; and
- there are adverse media reports or other relevant sources of information about the customer or its beneficial owner(s). For example, there are reliable and credible allegations of criminality, terrorism or proliferation against the customer or their beneficial owners. Relevant persons should determine the credibility of allegations on the basis of the quality and independence of the source data and the persistence of reporting of these allegations, amongst other considerations. Relevant persons should note that the absence of criminal convictions alone may not be sufficient to dismiss allegations of wrongdoing.

The customer's and the customer's beneficial owner's nature and behaviour

Though this is not specifically referred to in the Code, consideration should be given as to whether it is a relevant risk factor. Risk factors associated with a

customer's or their beneficial owner's nature and behaviour are below. Relevant persons should note that not all of these risk factors are apparent at the outset. They may only emerge once a business relationship has been established. They include, for example, whether:

- the customer has legitimate reasons for being unable to provide robust verification of identity;
- the relevant person has any doubts about the veracity or accuracy of the customer's or beneficial owner's identity;
- there are indications that the customer is seeking to avoid the establishment of a business relationship. For example, the customer wishes to carry out an occasional transaction or several occasional transactions, where the opening of an account with a relevant person might make more economic sense;
- the customer's ownership and control structure is transparent and makes sense or appears unnecessarily complex or opaque and whether there is an obvious commercial or lawful rationale for such structures;
- the customer provides vague or incomplete information about their proposed activities;
- the customer is reluctant to provide additional information about their activities when queried, e.g. as a result of negative news;
- the customer issues bearer shares or has nominee shareholders, where there is no obvious reason for having these;
- the customer is a legal person or legal arrangement used as an asset holding vehicle where beneficial ownership is not transparent;
- there are no apparent sound reasons for changes in the customer's ownership and control structure;
- the customer requests transactions that are complex, unusually or unexpectedly large or have an unusual or unexpected pattern without apparent economic or lawful purpose or a sound commercial rationale;
- the customer (or beneficial owner(s)) engages in or requests payments be made to third parties or third party destinations that do not accord with their stated business activities and/or where they are not party to the underlying transaction(s) being paid for;
- there are grounds to suspect the customer is trying to evade specific thresholds such as those set out under the Code's definition of exempted occasional transaction;
- the customer requests unnecessary or unreasonable levels of secrecy; for example, the customer is reluctant to share CDD information or appears to disguise the true nature of its business or requests, or tries to insist on, a Non-Disclosure Agreement;

- the customer's or beneficial owner's source of funds (or source of wealth where appropriate) cannot be easily and plausibly explained;
- the customer does not use products and services they have taken out as expected when the business relationship was first established;
- the customer is a non-resident whose needs could be better serviced elsewhere. For example, there is no apparent sound economic/lawful rationale for the customer requesting the type of financial service sought in the Isle of Man;
- the customer is insensitive to price or significant losses on investments; or
- the customer is a non-profit organisation whose activities put them at heightened risk of abuse for terrorist financing purposes.

Code 6(3)(c), (e), (g), 5(3)(d)

The manner in which the products and services are provided to the customer

This concerns how the business relationship/occasional transaction is conducted. It covers issues such as:

- the extent that the business relationship is conducted non-face-to-face;
- whether introducers or intermediaries are used and the nature of use;
- whether the customer themselves may be an undisclosed intermediary for a third party;
- where products, services or payments are to be provided to or from third parties; and
- the way technology is used in delivering products and services.

Code 6(3)(g), (e), 7(3)(d)

There is significant crossover of the considerations for this risk factor with other risk factors. Consequently, refer to guidance provided for:

- 6(3)(g) on whether the relevant person and the customer have met;
- 6(3)(e) on the involvement of third parties; and
- 7(3)(d) in respect of the TRA and the delivery of products and services.

Code 6(3)(d), 15(5), 15(7)

The risk factors included in paragraph 15(5) and (7)

The risk factors listed at paragraph 15(5) of the Code must be treated as higher ML/FT/PF risk and business relationships/occasional transactions where such matters are relevant must be treated as higher risk and subject to enhanced CDD.

The risk factors at paragraph 15(5) are considered in the context of geographic risk and customer reputation risk.

The risk factors listed 15(7) are matters that may pose a higher ML/FT/PF risk. Whether they in fact pose a higher risk is a matter for relevant persons to determine in the context of their BRA, CRA and TRAs. These risk factors are dealt with throughout the BRA, CRA and PEP guidance.

Coder 6(3)(c), (e), 5(3)(d), (e), 19(4)(g)

The involvement of any third parties for elements of the CDD process, including where reliance is placed on a third party

The Code specifies a number of situations where third parties can be involved in elements of the CDD process:

Code 9
- introduced business where a customer is introduced to a relevant person by a person (an Introducer) who provides elements of CDD (guidance regarding introduced business is at section 2.2.10);

Code 19
- eligibly introduced business where a customer is introduced to a relevant person by a third party who, per a terms of business, verifies the identity of customers (and any beneficial owners) and may be responsible for retaining the verification documents, data or information (guidance regarding eligibly introduced business can be found at 4.5);

Code 17, 12(2)(b),
- persons in the regulated sector acting on behalf of a third party, where there is no obligation for certain relevant persons to comply with paragraph 12(2)(b) of the Code (guidance regarding the concession where persons in a regulated sector acting on behalf of a third party concession can be found at 4.3);

Code 21, 12(2)(b)
- miscellaneous concessions where the relevant person is not required to comply with paragraph 12(2)(b) of the Code due to the status of parties related to the customer and expectations regarding CDD that accompany that status (guidance regarding the miscellaneous concessions can be found at 4.7); and

Code 22
- transfers of blocks of business from one relevant person to another where CDD on the business is provided to the purchaser by the vendor (guidance regarding the transfer of a block of business concession can be found at 4.8).

When any third parties are involved or relied on in the CDD process, relevant persons should consider the risks related to:

- how involvement or reliance is prompted and agreed;
- the extent and type of involvement/reliance on the third party(ies);
- who the third parties are, including:
  - their regulatory status;
  - any reputational issues, for example whether there are any indications that the third party's level of compliance with applicable AML/CFT/CPF legislation or regulation is inadequate, for example because the third party has been sanctioned for breaches of AML/CFT/CPF obligations;

Code 19(5)

- where the third party is part of the same financial group:
  - the extent that reliance can be placed on introductions as reassurance that the customers will not expose the relevant person to excessive ML/FT/PF risk;
  - the extent that the relevant person has taken measures to satisfy itself that the group entity operates AML/CFT/CPF programmes and procedures which conform to Parts 4 and 5 and paragraphs 33 to 37 of the Code;
  - the extent that the operation of those programmes and procedures is supervised at group level by an appropriate authority; and

Code 33, 34, 35, 36, 37, Part 4 ,5

- the group's AML/CFT/CPF policies adequately mitigate any risk associated with a jurisdiction for the time being specified on ~~List A~~List A or ~~List B~~List B;
- where the third party is not part of the same financial group:
  - what those third parties' main business activities are, whether those third parties are financial institutions, or their main business activity is unrelated to providing financial services;
  - whether the third party is a trusted person, a trusted person within the limits of paragraph 19(4)(f) or a person listed at paragraph 17(6) or 22(3) of the Code or none of the above;
  - whether the third party will provide, immediately upon request or otherwise required, relevant copies of CDD information, documents and data;
  - whether the quality of the third party's CDD measures is such that it can be relied upon;

Code 3(1), 9(4), 17(6), 19(4), 22(3)

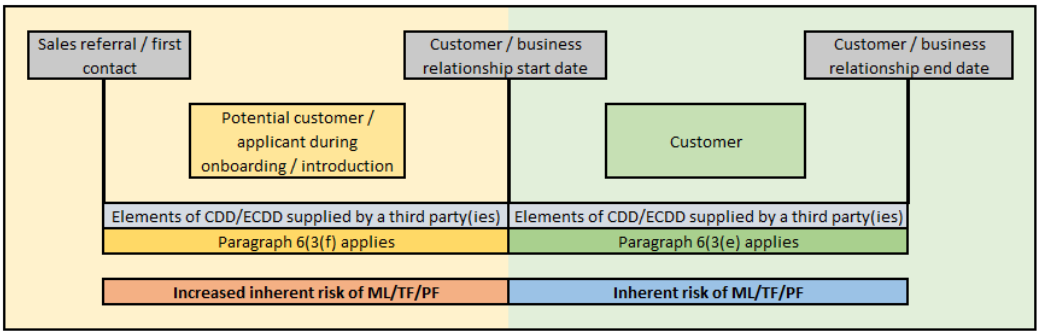
Code 19(7)

- the nature of the relationships with those third parties and whether they are longstanding and/or ongoing;
- the quality of relationships with those third parties and previous experience, for example:
  - the quality of CDD provided previously by the third party;
  - results of any testing undertaken on the third party's procedures;
  - responses to previous requests for documents, data or information; and
  - whether any issues have arisen with other customers where the third party has been involved for elements of the CDD process;

- geographic risks; the guidance provided on geographic risk for BRAs and CRAs at sections 2.2.8.3 and 2.2.9.2 is relevant when considering the geographic risks associated with third parties and can be used, subject to appropriate amendments;

- whether anyone, and if so who, has met the customer;
- the extent of any outsourcing undertaken by those third parties in respect of the CDD and the quality of providers used; guidance on outsourcing as a relevant risk factor can be found at sections 2.2.8.3 and 2.2.11.2; and
- the nature of the relationship between any third party and the customer and the extent that any third parties are involved on an ongoing basis in the conduct of business relationships with customers and whether and how this affects the relevant person's knowledge of those customers and ongoing risk management.

Specific risk factors and considerations are also provided at section 2.2.10.4 on the introducer risk assessment.



To assist with considering whether a third party should be considered under either 6(3)(e) or 6(3)(f) of the Code, firms may find the above diagram of use.

Code 6(3)(f), 9(4)

Any risk assessment carried out under paragraph 9(4) – Introducer Risk Assessment

Where a customer is introduced in accordance with paragraph 9 of the Code, the CRA must be supplemented with the risk assessment requirements of paragraph 9(4). This requires an introducer risk assessment, as well as consideration of specific factors relating to the introduction. Guidance on introducer risk assessments is at section 2.2.10.

Code 6(3)(g), (c), 5(3)(d)

Whether the relevant person and the customer have met during the business relationship, or its formation, or in the course of an occasional transaction.

Meeting a customer is part of the process of establishing that a person exists and that the person the relevant person is dealing with is who they say they are. When a customer has not been met, the CDD paper trail may be correct in that it flowed from the customer, but there is a risk that the CDD is incomplete, inaccurate and/or may not accurately reflect the customer. This may also be the case where the customer has been met by an unreliable third party.

When considering this risk factor, relevant persons will need to have clearly established policies and procedures as to what it means, in their view, to meet a customer. This is both in respect of methods used to meet a customer and, where

a customer is a non-natural person, in determining which natural persons should be met in any particular case.

Code 4(2), 5, 6, 7

One method of meeting a customer is for the customer to be physically present. However, in the digital age, being physically present is not necessarily the only method of meeting a customer. Whether the relevant person considers it appropriate to use other methods and what other methods they consider appropriate in any particular instances or cases will depend on the outcomes from the BRA, TRA and CRAs. For relevant persons that may require further assistance, the Authority's Supplemental Information Document, provides information in relation to verification of identity and address which includes an example method for meeting a customer using technology.

Where a customer is a non-natural person[9], considerations when determining which natural persons to meet would include:

Code 12

- the natural persons listed at paragraph 12 of the Code to be identified and their identity verified (see section 3.4.5 of the CDD chapter); and,
- where there are multiple signatories/directors, the considerations set out at section 3.6.2.

Relevant persons must be mindful of the overarching obligation that their procedures and controls must enable them to manage and mitigate their ML/FT/PF risks.

Code 15(7)(k)

Paragraph 15(7)(k) of the Code notes that where the relevant person and the customer have not met during the business relationship or during its formation, or in the course of an occasional transaction, in certain circumstances this may pose a higher ML/FT/PF risk.

Considerations when assessing this risk factor should include:

- whether the customer is/was physically present or has been met using other methods the relevant person has determined are appropriate (subject to the relevant risk assessments) for identification purposes. If they are/were not physically present/otherwise met, whether the relevant person:
  - considered whether there is a risk the customer deliberately sought to avoid face-to-face contact for reasons other than convenience or incapacity;
  - whether the relevant person uses reliable forms of non-face-to-face CDD; and

[9] For further guidance please see the TCSP AML/CFT Sector Specific Guidance Section 4.1. It should be considered who is being "met" in order to determine if the customer has been "met" i.e. is it the directors of the TCSP that has created the entity or is it the person(s) who have actually had the structure created, which would be a better representation of who the customer actually is.

- the extent that the relevant person has taken steps to prevent impersonation or identity fraud.
- the extent that the business relationship is conducted on a non-face-to-face basis.

2.2.10 The broader CRA – the Introducer risk assessment

Code 9(3), (4), 6

9 Introduced business

(3) The relevant person must carry out a customer risk assessment in accordance with paragraph 6 and sub-paragraph (4).

Code 9 (3)

The introducer risk assessment is an add-on to the CRA where a customer is introduced to a relevant person by a person who provides elements of the CDD. This is to address the potentially increased ML/FT/PF risk of accepting customers introduced by a third party (introducer) that provides elements of their CDD.

Code 9(4)

Where elements of CDD provided by the introducer have been provided by a third party, the introducer risk assessment also requires the relevant person to consider the role and standing of other third parties that may have met the customer or been involved in the CDD process.

Code 6(2)

The requirements at paragraph 6(2) with respect to the timing, recording and review of the CRA apply to the introducer risk assessment as they do to the rest of the CRA. However, due to the particular circumstances of introduced business situations, additional guidance is given which is supplemental to the general guidance and should be read in conjunction with and not in isolation from it.

2.2.10.1 Introducer risk assessment reviews

Code 9(3), 6(2)(c)

As with the standard CRA, this broader CRA incorporating an introducer risk assessment and third-party considerations should be viewed as a living document that is regularly revisited, reviewed and amended to keep it up to date.

The introducer risk assessment and third-party considerations are not conducted in isolation but are integral to the CRA. Consequently, information may come to light about the introducer/third parties when taking on an introduced customer that affects the relevant person's views on that customer and/or on previously introduced customers. Conversely, relevant persons should be mindful that during the course of a customer relationship, information may come to light about an introduced customer that affects the relevant person's view of the introducer and other third parties that are or were involved in the customer introduction. This may have a ripple effect on other customers introduced by that introducer, or with connections to those third parties.

Code 4(6)(2)

It is for relevant persons to determine the depth and frequency of reviews of the broader CRA. Documented considerations in determining the depth and frequency include the following:

- The relationship between the relevant person and the introducer/third parties, and the role adopted by the introducer. For example, the risk assessment for an introducer who only provides elements of CDD for a one-off introduction and has no further involvement in the customer's dealings with the relevant person may never need to be reviewed. Whereas the risk assessment for an introducer who provides elements of CDD for regular customer introductions may need to be reviewed more frequently. This should be determined on a case-by-case basis and will be affected by the information already held, previous risk assessments and new information arising from later customer introductions.

2.2.10.2 Recording the introducer risk assessment

Code 9, 6(2)(b)

As with the standard CRA, the broader CRA encompassing the introducer risk assessment must be recorded in order to be able to demonstrate its basis.

How a relevant person chooses to document and organise the additional elements of the broader CRA should be determined on a case-by-case basis. In some cases, it may be appropriate for the additional elements to be documented as part of the relevant CRA. Alternatively, for example where an introducer has introduced several customers, relevant persons may find it more helpful to have a centralised introducer risk assessment file which is linked to the relevant customer files. If a relevant person chooses to complete centralised introducer risk assessments these do not need to be updated every time a piece of new business is received from that introducer. However, every CRA must include consideration of the introducer risk assessment (e.g. whether the piece of business received from the introducer is in line with expected business from that introducer).

Whatever system of organisation is used, relevant persons must be able to relate the additional introducer and third-party specific elements of the CRA to the relevant customers and vice versa on an ongoing basis.

2.2.10.3 Timing of the introducer risk assessment

Code 9 (3), 6(2)(a)

The timing of the introducer risk assessment is as per the CRA, because the introducer risk assessment is simply a supplementary element to it. Consequently, it must be undertaken prior to the business relationship being established or an occasional transaction carried out.

2.2.10.4 Relevant risk factors specific to the introducer risk assessment

The broadened CRA must include and take into account all of the following factors:

Code 9(4)

9 Introduced business

(4) The risk assessment must include and take into account –

(a) a risk assessment of the introducer;

(b) whether the introducer has met the customer;

(c) whether any elements of customer due diligence provided by the introducer have been obtained by the introducer –

(i) directly from the customer; or

(ii) from any third parties; and

(d) if sub-paragraph (4)(c)(ii) applies, indicate –

(i) how many third parties were involved in the process;

(ii) who those third parties were;

(iii) whether any of those third parties have met the customer;

(iv) whether any third party is a trusted person; and

(v) whether in the case of any third parties located outside of the Island, they are located in a List C jurisdiction.

Code 6(3)(e)

This guidance on the broadened CRA should be read in conjunction with, and not in isolation from, the guidance at section 2.2.9 on the CRA and the Code 6(3)(e) risk factor.

Code 9(4)(a)

(a) a risk assessment of the introducer

The purpose of an introducer risk assessment is to:

- enable relevant persons to estimate the ML/FT/PF risk posed by a customer taken on by way of an introduction;
- enable relevant persons to determine the extent, if at all, that they can reasonably rely on elements of customer CDD provided by the introducer;
- determine whether reliance on elements of CDD provided by an introducer increases the ML/FT/PF risk associated with the customer. If the customer is assessed as higher risk, enhanced CDD must be undertaken.

Code 9(4)(a), 6(3)(e)

When undertaking/reviewing an introducer risk assessment, considerations additional to those listed for the CRA in respect of Code paragraph 6(3)(e) include, but are not limited to:

- the extent, and the particular elements, of CDD provided by the introducer;
- whether the introduction seems in line with the usual types/profiles/patterns of customers the introducer has previously introduced to the relevant person (if applicable);
- what processes the introducer goes through when introducing customers (i.e. if they meet the customer) and whether/how these processes change according to the particular circumstances.

Code 9(4)(b), 6(3)(g)

(b) whether the introducer has met the customer

The guidance given for the CRA risk factor at Code paragraph 6(3)(g) (whether the relevant person has met the customer) is relevant in respect of this introducer risk assessment risk factor.

Where the relevant person is determining whether an introducer has met the customer the relevant person will need to understand what "meeting the customer" means to the introducer and whether the processes and procedures they have followed in any particular case would satisfy the relevant person's own policies and procedures for meeting a customer.

It is important that the relevant person understands who exactly, if anyone, has met the customer, by what means the customer has been met and, where a customer is a non-natural person, which natural persons associated with the customer (if any) have been met, in order to properly assess the customer risk.

Code 9(4)(c)

(c) whether any elements of customer due diligence provided by the introducer have been obtained by the introducer –

(i) directly from the customer; or

(ii) from any third parties.

This requires further consideration of the completeness, accuracy and reliability of CDD obtained by the introducer. The introducer may have obtained some or all of the CDD directly from the customer, but may also have obtained some or all of that CDD from a third party who subsequently introduced the customer to them. It is important to determine what proportion, and which elements, of the CDD have been obtained by the introducer directly from the customer and which from third parties. Where CDD is not obtained directly from the customer, there is an increased risk that it may be inaccurate or incomplete.

Code 9(4)(d)

(d) if sub-paragraph (4)(c)(ii) applies, indicate –

(i) how many third parties were involved in the process;

(ii) who those third parties were;

(iii) whether any of those third parties have met the customer;

(iv) whether any third party is a trusted person; and

(v) whether in the case of any third parties located outside of the Island, they are located in a List C jurisdiction.

If elements of CDD have been obtained by the introducer from third parties rather than directly from the customer, the relevant person must assess, as part of the CRA, the extent of involvement of third parties in the transfer of CDD from the customer to the introducer and thus on to the relevant person. It is important that the relevant person fully understands the conduit chain from the customer to the introducer. Code paragraph 9 specifically requires the CRA to include an indication of the factors listed below.

- **How many third parties were involved in the process** – the relevant person must understand how many layers there are in the chain leading up to the introducer. Each layer has the potential to distance

the relevant person from their customer and potentially increases the risk that the CDD provided is inaccurate or incomplete or that the customer may not be who they claim to be.

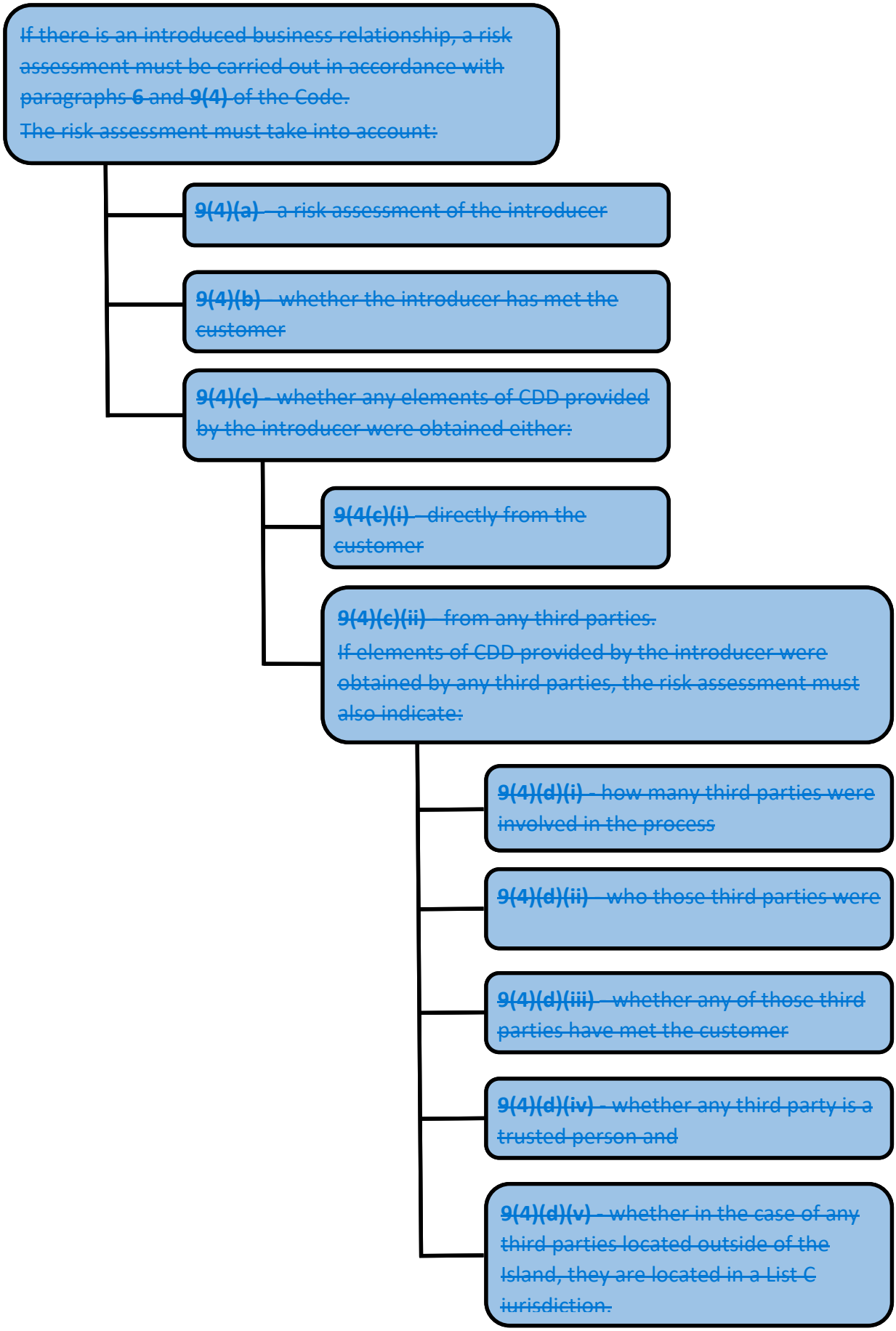
- **Who those third parties were** – the relevant person must understand who the third parties involved in the chain leading up to the introducer were and what their role was. Relevant factors to consider include:
  - whether a third party actually gathered any elements of CDD or simply acted as a link in the chain;
  - what activities the third parties undertake;
  - whether a third party is known by/has had dealings with the introducer and/or the relevant person previously and in what context;
  - whether any of those third parties met the customer; and
  - the reputation of the third party.

Code 9(4)(d), 3(1)

- **Whether any third party is a trusted person** – trusted persons are subject to AML/CFT/CPF compliance requirements at least equivalent to those in the Code and are supervised or overseen for compliance with the same, either in the Isle of Man or in a List C jurisdiction. If a third party is not a trusted person, they may not be subject to sufficient, or indeed any, regulatory oversight to ensure that any CDD they gather or transmit is complete, accurate or trustworthy. Consequently, involvement of third parties that are not trusted persons in the process may indicate increased ML/FT/PF risk and should be treated more cautiously.
- **Whether in the case of any third parties located outside of the Island they are located in a ~~List C~~List C jurisdiction**

A flow diagram to assist relevant persons with the broadened risk assessment requirements is below.

Determining what should be in the broadened risk assessment



2.2.11 Technology risk assessment ("TRA")

Code 3(1)

3 Interpretation

(1) In this Code -

"technology risk assessment" has the meaning given in paragraph 7 (technology risk assessment) and includes both new and developing technologies;

Code 7(1)

7 Technology Risk Assessment

(1) A relevant person must carry out an assessment that estimates the risk of ML/FT posed by any technology to the relevant person's business.

Code 4(3)

The particular purpose of the TRA is to ensure relevant persons fully understand the ML/FT/PF risks from any technology, and the impact any technology may have on the relevant person's compliance with AML/CFT/CPF requirements. This will help relevant persons comply with their AML/CFT/CPF obligations irrespective of the technology used.

The TRA requires relevant persons to focus detailed attention on a complex and dynamic area tailored to the particular ML/FT/PF risks faced by their business. Innovations in technology can improve the effectiveness and efficiency of AML/CFT/CPF measures, but there is also the risk that they weaken such measures where they are applied badly or without sufficient consideration and understanding.

Code 7(2)(b)

Where new products, services, business practices delivery methods/systems are introduced by a group which affect the relevant person, the relevant person must ensure the group's AML/CFT/CPF risk assessment of the technology is sufficiently granular and specific to meet the needs of the relevant person in order that they can manage and mitigate their ML/FT/PF risks. If the group's risk assessment is not sufficient to enable the relevant person to comply with the Code, the relevant person must perform its own TRA prior to using, launching or implementing new offerings, practices, technologies etc.

Relevant persons should note that the TRA concerns any technology that may pose ML/FT/PF risks to the relevant person. The TRA is not limited to new technologies used by the relevant person and it is not limited to technologies used in the CDD process.

2.2.11.1 Timing of the TRA

Code 7(2)

7 Technology Risk Assessment

(2) The technology risk assessment must be –

(a) Undertaken as soon as reasonably practicable after the relevant person commences business;

(b) Undertaken prior to the launch or implementation of new products, new business practices and delivery methods including new delivery systems;

(c) Undertaken prior to the use of new or developing technologies for both new and existing products;

Code 4(1) All existing relevant persons must already have undertaken a TRA. Newly licensed or registered relevant persons must undertake the TRA before entering into or carrying on a business relationship/occasional transaction.

Code 7(2)(b) Subsequent to the first TRA, a TRA must also be undertaken before the relevant person launches or implements new products, business practices and delivery methods/systems.

Code 7(2)(c) Relevant persons must also undertake a TRA before new or developing technologies are used for both new and existing products because the ML/FT/PF risks may not be the same for new and existing products.

These requirements reflect the dynamic and innovative nature of technology in business offerings and solutions in all areas of a business which can impact AML/CFT/CPF controls and that the ML/FT/PF risks change and evolve as a result of these changes and as technology matures.
The TRA should be considered a live document integral at the outset to the development and decision making process for any new products or services, business practices, delivery methods/systems, use of new/developing technologies for new and existing products. Consideration of ML/FT/PF risks should be a primary concern when developments are being made in these areas and not an afterthought once the developments are in their final stages.

Code 7(2) The requirement to complete a TRA before such changes is in addition to the requirement to regularly review the TRA and keep it up-to-date.

2.2.11.2 Relevant risk factors

Code 7(3), 5

7 Technology Risk Assessment

(3) The technology risk assessment must have regard to all relevant risk factors including –

(a) Technology used by the relevant person to comply with AML/CFT legislation;

(b) The business risk assessment carried out under paragraph 5;

(c) The products and services provided by the relevant person;

(d) The manner in which the products and services are provided by the relevant person, considering delivery methods, communication channels and payment mechanisms;

(e) Digital information and document storage;

(f) Electronic verification of documents; and

(g) Data and transaction screening systems.

New technologies expose relevant persons to ML/FT/PF risks similar to those associated with current business practices, but with particular technology relevant nuances that relevant persons need to take into account. As a consequence, the considerations listed in respect of the BRA and the CRA may also be relevant (particularly with respect to products and services and the manner that products and services are provided) when considering the equivalent TRA risk factors. To avoid unnecessary repetition risk factors and considerations expounded under the BRA/CRA are not reiterated here.

Considerations which are common to all TRA relevant risk factors include:

- the extent to which the relevant person (or their financial group) is at the leading edge of new and evolving technologies; conversely, the extent that the relevant person prefers to wait to adopt new technologies until the technology matures;
- the extent that new technologies mitigate existing ML/FT/PF risks and/or increase the effectiveness and efficiency of existing AML/CFT/CPF measures;
- the extent that new technologies expose the relevant person to new ML/FT/PF risks;
- the extent that, when new business practices, offerings or delivery methods and systems are implemented, existing technology, which may not itself change, may become more vulnerable to ML/FT/PF risks;
- the extent that new technologies are part of a relevant person's core infrastructure;
- how well new technologies interface seamlessly with legacy infrastructure;
- the robustness of the technology including where and how weaknesses in the technology arise, the potential for failures in the technology and its ability to withstand cyber-attack;
- the extent and results of testing technologies for:
    - robustness, and the adequacy of controls to mitigate potential risks and the robustness of the business continuity plan;
    - compliance with the AML/CFT/CPF requirements and the relevant persons' procedures and controls; where testing is inconclusive, relevant persons should maintain their traditional systems parallel to the new technology until they have full confidence in that technology. where serious weaknesses are identified, relevant persons should re-evaluate:
        - whether the technology's level of reliability is justifiable against the ML/FT/PF risks;
        - the need to improve the technology;

        - whether it is appropriate to continue to use the technology.
    - assurance levels associated with any technology including what the assurance covers and who provides the assurance (such as those associated with digital identity systems);
    - supplier/outsourcing risks where technology is sourced from external vendors, considerations include:
        - geographic risks;
        - connected persons risks;
        - supplier maturity;
        - risk of irreparable system failure;
        - likelihood of technology becoming obsolete and the transferability of data in that event;
        - registration with relevant data protection authorities;
        - accreditation/certification with government/industry bodies that require certain standards to be met;
    - where technology is sourced from external suppliers, sufficiency of in-house expertise to guarantee the implementation and use of the technology and ensure the continuation of business practices, controls, products, services and delivery methods/systems in the event of system failure, data loss, cyber-attack or termination of the business relationship between the relevant person and the external vendor;
    - the extent that senior management and other relevant staff have appropriate understanding of the technology, including its objective and what it does or does not do, its strengths and its potential/actual weaknesses;
    - barriers to information sharing between external providers of technology and the relevant person, and/or between the external provider and a competent authority, where external providers are based in a third country;
    - financial inclusion considerations (guidance regarding financial inclusion is at section 3.3.5); and
    - connectivity issues.

Code 7(3)(a)

(a) Technology used by the relevant person to comply with AML/CFT legislation

Code 3(1)

3 Interpretation

(1) In this Code -

"AML/CFT legislation" means the requirements of –

(a) sections 7 to 11 and 14 of the Anti-Terrorism and Crime Act 2003;

(b) Part 3 of the Proceeds of Crime Act 2008;

(c) Parts 2 to 4 of the Terrorism and Other crime (Financial Restrictions) Act 2014;

(d) financial sanctions which have effect in the Island; and

this Code,

The TRA must have regard to technology used to comply with all AML/CFT/CPF requirements and not only those of the Code. In addition to the common considerations listed above, other considerations include:

- the extent to which the relevant person retains sufficient decision making powers with respect to proposed changes to the technology, for example in respect of the applicable CDD measures, monitoring parameters, or unusual/suspicious indicators;
- processes in place to ensure continuous monitoring of the technology's reliability and effectiveness; the extent to which technology used is regularly assessed with errors/weaknesses corrected without delay;
- controls to reduce the risk of collusion between staff and customers.
- in respect of technological solutions to CDD requirements, considerations include whether:
    - the technology is sufficiently reliable and commensurate with the level of ML/FT/PF risks per the BRA and CRA of individual business relationship/occasional transactions;
    - there is a risk the customer's image visible on the screen is being tampered with during the transmission.
    - there is a risk that an ID document displayed on the screen by a customer belongs to another but similar looking person.
    - multiple sources are used including positive sources and negative information sources such as fraud and deceased persons records;
    - data sources are kept up to date;
    - processes are transparent allowing the relevant person to see what checks are carried out, the results of those checks and what they mean; and
    - relevant persons are able to capture and store the information used; and
- controls to ensure relevant staff (including staff of an external provider) using technology are sufficiently trained with particular focus on the practical application of the technology including:
    - its technical abilities and limitations. For example, in the case of technology used to verify identity, ensuring a full understanding of the checks undertaken by the technology, the checks not undertaken and the results of those checks to enable a determination of the level of satisfaction provided by those checks (guidance regarding the use of electronic methods for CDD can be found at section 3.3.4.5); and
    - its relevance in the detection and escalation of potentially suspicious activities arising from the use of the technology.

Code 7(3)(b)

(b) The business risk assessment carried out under paragraph 5

The findings of the BRA should inform the TRA.

Code 7(3)(c), 5

(c) The products and services provided by the relevant person

The ML/FT/PF risks/considerations associated with a relevant person's products, services and associated transactions listed in respect of the BRA are, when adjusted relative to the technologies used by the relevant person, applicable to the TRA. To avoid unnecessary repetition, they are not repeated in full here, though in brief they include:

- the level of transparency, or opaqueness of the products, services or transactions;
- the complexity of the products, services and transactions; and
- the value or size of the product, services or transactions.

The common TRA considerations listed above would also apply.

Code 7(3)(d)

(d) The manner in which the products and services are provided by the relevant person, considering delivery methods, communication channels and payment mechanisms

In addition to the common considerations listed above, other considerations include:

- the appropriateness and extent of technologies moving from human trust frameworks to algorithm based trust models, (for example where block chain or other distributed ledger technology is used). Relevant persons should consider whether, and the extent to which, ML/FT/PF risks, previously managed and mitigated by central/human intermediaries, are mitigated by new technology. should not rely entirely on new technology and will need to apply human judgement to outputs from new technology; and
- the attractiveness of faster transaction times which accompany new technologies for ML/FT/PF.

Code 7(3)(e)

(e) Digital information and document storage

In addition to the common considerations, other considerations include:

- whether the technology enables the relevant person to comply with their obligations to record, retain and retrieve records required by the Code, or whether other controls are required;
- whether the technology enables the relevant person to determine the receipt date and applicable document retention periods for documents, data and information obtained under the Code requirements;
- risk of data loss; and

- the adequacy of controls in place to ensure compliance with data protection and privacy requirements.

Code 7(3)(f)

(f) Electronic verification of documents

In addition to the common considerations and considerations in respect of technology used to comply with AML/CFT/CPF legislation, other considerations include:

- risk that a document has been tampered with or forged (e.g. tampered or forged pictures, or security features such as holograms or watermarks);
- risk that copies of documents or photographs have been tampered with before transmission (e.g. the use of software to alter data or photographs);
- risk of falsified documents being used; and
- risk of stolen documents being used.

Code 7(3)(g)

(g) Data and transaction screening systems

In addition to the common considerations, other considerations include:

- whether the technology can be/is integrated with the relevant person's existing workflows and legacy systems. In order for technology to be effective and efficient for ongoing monitoring purposes, it should be fully integrated with the relevant person's current and legacy systems and should have full access to all available information about the relevant person's customers across multiple accounts (current and historical) and networks;
- whether the relevant person is able to determine what data and information sources are used in the ongoing monitoring process and assess its reliability;
- the technology's ability to develop a sufficiently informed view of which transactions should be considered potentially suspicious or unusual. As views on unusual/suspicious activity are based on historical data, patterns of transactions and previous suspicious activity reports, this will be affected by the level of data completeness;
- whether the technology enables the relevant person to develop a holistic view of their customers' profiles including their transactions/activity, links between customers/entities/payments etc. Linking customers' transaction patterns with static data held in relevant person's databases and information from other multiple data sources (such as government registers, device/machine fingerprinting, online news and publications, social media and public databases and registers); and
- the controls in place to ensure CDD documents, data or information obtained using new technology remains accurate and up to date and

relevant persons remain compliant with their obligations under the Code.

3. Customer due diligence, ongoing monitoring and enhanced measures

3.1 Purpose of customer due diligence ("CDD") and enhanced measures

Code Parts 4, 5

The purpose of CDD and enhanced CDD ("ECDD") in the AML/CFT/CPF context is to ensure relevant persons know, as far as reasonably possible, who they are dealing with and the ML/FT/PF risks of dealing with that customer. Robust CDD/ECDD procedures ensure relevant persons have their eyes wide open to the potential ML/FT/PF risks posed by any and all of their customers at the outset and for the duration of the business relationship/occasional transaction.

It is only with robust CDD/ECDD procedures that relevant persons are able to forestall abuse of the financial system by criminals or by those who would seek to use it for terrorism purposes. It is only with robust CDD/ECDD procedures that relevant persons can meet the requirements of all other AML/CFT/CPF legislation, not just the Code, effectively. CDD/ECDD is integral to managing and mitigating ML/FT/PF risks, since without satisfactory CDD/ECDD, it is impossible to conduct effective risk assessments, monitor business relationships/transactions for unusual or suspicious activity or make meaningful and comprehensive disclosures of suspicions to the IOMFIU.

POCA s 4

CDD/ECDD also:

- helps protect the relevant person and the integrity of the Isle of Man regulated sectors (per Schedule 4 of POCA) by reducing the likelihood of

relevant persons becoming a vehicle for, or victim of, other financial crime;
- assists law enforcement by providing available information on customers or activities, funds or transactions being investigated; and
- helps to guard against identity theft.

Code 33, 35, 35

Similarly, it is only by (per paragraphs 33-35 of the Code) adequately documenting the CDD/ECDD steps and analysis that has been undertaken, as well as the reasoning behind those steps, or the documents, data or information obtained as part of the CDD/ECDD process, that relevant persons can satisfy the AML/CFT/CPF legislation and demonstrate their ongoing compliance. Guidance on record keeping is in section 6.4.

Code 8(5), 9(9), 10(5), 11(7), 12(11), 14(6), 15(8), 19(11)

It is due to the CDD/ECDD requirements' utmost importance to AML/CFT/CPF efforts that where the CDD/ECDD requirements cannot be met, the business relationship/transaction must proceed no further/be carried out. Depending on the specific Code requirement, the relevant person must either terminate or consider terminating the business relationship and consider making an internal disclosure (see section 5.4).

3.2 Definitions

All terms used in this part of the Handbook are as defined in the Code, where a Code definition is provided. Some of the key terms, including some of those where there is no Code definition, are explained further below.

3.2.1.1 Customer due diligence ("CDD")

Code 3(1)

3 Interpretation
(1) In this Code -
"customer due diligence" (except in the expression **"enhanced customer due diligence"**) means the measures specified in paragraphs 8 to 14, 16 to 22, 36, 37, and 39 for the purposes of identifying and verifying the identity of customers, any beneficial owners and other persons;

Code 13

Conducting 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. Elements of this information must also be verified. CDD incorporates the ongoing monitoring of a business relationship, including the due diligence information obtained, to ensure it remains up to date, accurate and appropriate and that the relationship is operating as expected for that customer. CDD is required for all new or continuing business relationships and occasional transactions.

3.2.1.2 Identification and Verification ("ID&V")

Code 8 – 12, 15 - 22

The terms "identity" and "identification" are not defined in the Code. ID&V falls within CDD, and is the concept of being satisfied that the customer (or whoever

or whatever you are dealing with) is who they say they are. ID&V requirements apply to customers as well as other persons specified within the Code. But for the sake of explaining what is meant by ID&V this passage will only refer to customers.

It is important to distinguish between identifying the customer and verifying identification information. Identification requires information to be obtained about a customer's identity. This enables the relevant person etc. to know who the customer is. At this stage, no identification documentation is collected. Whereas, verification of the customer's identity, requires checking independent, reliable source documents, data or information to confirm the veracity of the identifying information obtained during the identification process.

Code 4(2)

Exactly what information is obtained and subsequently verified and how it is verified will vary on a case-by-case basis relative to ML/FT/PF risk provided the procedures enable the relevant person to manage and mitigate their ML/FT/PF risks.

Code Part 6

Exactly who obtains the information and verifies it will also vary on a case-by-case basis in accordance with the use of any Code concessions.

Guidance on identification and verification of identity is at sections 3.5 and 3.6. Guidance on Code concessions is in chapter 4.

3.2.1.3 Reasonable measures

Code 3, 8, 9, 11, 12, 14-20, 22, 42

The term "reasonable measures" is used throughout the Code and allows flexibility. What constitutes "reasonable measures" is relative to the relevant person's circumstances and the business relationship / occasional transaction concerned.

Code 4(2)

Relevant persons must take a risk based approach which accounts for higher risks when determining what measures are reasonable. The measures taken must enable the relevant person to manage and mitigate their ML/FT/PF risks.

This approach acknowledges that, for example, it may not always be possible to verify the identity of beneficial owners absolutely, but taking reasonable measures to verify their identity is possible.

In the context of source of funds and source of wealth, "taking reasonable measures to establish" is detailed further in the source of funds and source of wealth section at 3.8.

3.2.1.4 Enhanced customer due diligence ("ECDD")

Code 3(1), 13, 14(3), 15

3 Interpretation
(1) In this Code –
"enhanced customer due diligence" means the steps specified in paragraph 15 (enhanced customer due diligence) which are additional to the measures specified

in paragraphs 8 to 14, 16 to 22, 36, 37 and 39 for the purpose of identifying and verifying the identity of customers, any beneficial owners and other persons;

Code 15(2), (3)

ECDD means taking specified steps additional to the standard CDD requirements in respect of a new business relationship, occasional transaction or continuing business relationship. ECDD is required where there are higher risks or unusual activity. ECDD must also be undertaken in the event of any suspicious activity, unless the relevant person reasonably believes conducting ECDD will tip off the customer. ECDD requirements include establishing the source of wealth, undertaking further research on a customer's background and considering what additional identification information and verification should be obtained and ongoing monitoring carried out.

Guidance on ECDD is at section 3.4.7.

3.2.1.5 Ongoing monitoring

Code 13

Ongoing monitoring means examining all aspects of the business relationship including the CDD / ECDD already obtained as well as the customer's activity. It should focus on any changes in transactions or activities, and in particular any transaction or activity that is not in line with the customer's expected activity. These transactions and activities should be scrutinised more thoroughly.

Code 4(1)

Appropriate screening for sanctions listings and negative press should also be undertaken, as well as further open source internet searches undertaken as necessary.

Code 13(4), 4(2)

The extent and frequency of ongoing monitoring must be risk based and enable relevant persons to effectively manage and mitigate their ML/FT/PF risks.

Guidance on ongoing monitoring is at section 3.4.6.

3.2.1.6 Enhanced Ongoing Monitoring

Code 15(2)(e), 14(4), 13, 4(2)

Enhanced ongoing monitoring falls within the requirements of ECDD. It means that where there are higher ML/FT/PF risks, including in respect of relationships with foreign PEPs and domestic PEPs who have been identified as posing a higher ML/FT/PF risk, relevant persons must consider what additional monitoring should be undertaken and carry it out in order to effectively manage and mitigate these higher risks.

Guidance on enhanced ongoing monitoring is at section 3.4.7.

3.3 Key principles of CDD

3.3.1 Ultimate responsibility for compliance with CDD requirements

Code 4(3)

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.

Code 4(3), 42

Relevant persons must always be mindful that though it may be possible to rely on third parties for certain aspects of CDD, or outsource certain practical CDD steps to others, it is not possible to outsource responsibility for compliance with any of the Code's requirements. The offences at Code paragraph 42 apply to the relevant person and any officer or partner (where relevant) where the relevant person has contravened the Code's requirements. Relevant persons should therefore ensure they are satisfied that, where they place reliance on a third party by whatever means, the requirements of the Code are met.

3.3.2 Anonymity is unacceptable

Code 40

40 Fictitious, anonymous and numbered accounts
A relevant person must not set up or maintain an account in a name that it knows, or has reasonable grounds to suspect, is fictitious, an anonymous account, or a numbered account for any new or existing customer.

The requirement at paragraph 40 applies to both new and existing customers.

Where historic numbered accounts exist, relevant persons must maintain them in such a way as to ensure full compliance with their legal obligations. Relevant persons must properly identify and verify the identity of the customer per the Code and be able to demonstrate compliance when requested by a competent authority.

Code 25(d)

In all cases, whether the relationship involves numbered accounts or not, the CDD records must be available to the MLRO, Head of Compliance/Compliance Officer, other appropriate staff and competent authorities.

Equally, relevant persons should note that non-disclosure agreements do not allow relevant persons to fail to or refuse to meet Code requirements (including risk assessments, CDD and record keeping). Nor do they allow relevant persons to fail to provide relevant information on the customer or any beneficial owner(s) when asked or required by a competent authority.

3.3.3 Risk based approach

Code 4(2)

A risk based approach to CDD procedures and controls is not optional, it is required by virtue of paragraph 4(2).

4 Procedures and Controls
(2) The Procedures and controls referred to in sub-paragraph (1) [including CDD procedures] must –

(a) have regard to the materiality and risk of ML/FT including whether a customer, introducer or eligible introducer poses a higher risk of ML/FT;

(b) enable the relevant person to manage and mitigate the risks of ML/FT that have been identified by the relevant person when carrying out the requirements of the Code;

(c) be approved by the senior management of the relevant person.

Code 4(2), 5, 6, 7

CDD procedures must flow from the BRA, CRAs and TRA. Relevant persons should use the findings from the BRA to inform the CDD procedures that will be applied to individual business relationships and occasional transactions. Relevant persons must apply CDD measures in all cases, but the extent of such measures may be adjusted relative to the ML/FT/PF risk in any particular case. It is for relevant persons to determine what is appropriate to their circumstances.

Code 4(2), 6 8(2), (4), 11(2), 14 – 22

CDD measures and CRAs are in a continuous feedback loop. Initial CDD must be undertaken before a business relationship/occasional transaction is entered into or during the formation of that relationship. This initial CDD allows relevant persons to undertake an initial CRA. This initial CRA enables relevant persons to determine whether the initial CDD obtained is sufficient for that business relationship/occasional transaction, and adjust the extent of CDD needed for that individual business relationship/occasional transaction. Where the risks associated with a business relationship/occasional transaction are higher, the Code requires enhanced measures to combat ML/FT/PF. Where the risks are lower, and any conditions are met, the Code allows exemptions and simplified measures, as well as flexibility in how CDD measures are applied. This means that the amount and type of information obtained, and the extent to which this information is verified must be increased where the risk is higher and may be simplified where the risk is lower. The procedures and controls adopted must enable relevant persons to effectively manage and mitigate their risks, including where there are higher risks.

Code 4(1), (2), 30(1), 32

Relevant persons must ensure staff are familiar with their relevant policies, procedures and controls. This includes ECDD measures where there are higher risks. Relevant persons should maintain their own lists of source documents, data and information they will accept in each case. Such lists, forming part of the relevant person's procedures and controls, must be monitored to ensure they remain acceptable and fulfil the relevant person's needs. A risk sensitive approach to such documents, data and information and an understanding of its limitations is essential in ensuring relevant persons are able to manage and mitigate their ML/FT/PF risks effectively. Examples are provided within the Supplemental Information Document, but these are not exhaustive, nor should they be considered limited. It may be, that according to the relevant person's circumstances and the results of the risk assessments, more information, documents or data is required to ensure they effectively manage and mitigate

their risks. Whatever methods are used, the primary objectives of ensuring the relevant person knows its customer and can manage and mitigate its ML/FT/PF risks remain.

3.3.4 Reliability and independence of source documents, data or information

Code 8(3), 9(7), 10(3), 11(3), 12(2), 12(6) – (10), 15(2), 17(2), 18(3), 19(4), 19(7), 20 (4)

When undertaking CDD procedures, relevant persons must use reliable and independent source documents, data or information (whether or not in hard or electronic form). The Code does not define what reliable and independent source documents, data or information is. This means that relevant persons have some flexibility regarding the sources used to meet CDD obligations. In addition, both the Code and this guidance are technology neutral, so provided a relevant person can demonstrate the sources used enable them to comply with their CDD obligations and are commensurate with the ML/FT/PF risks posed by the business relationship/occasional transaction, relevant persons can use alternative sources such as new technologies and innovative solutions.

To be satisfied of the reliability and independence of such sources requires relevant persons to understand their inherent strengths and limitations as well as the strengths and limitations arising as a result of the way the documents, data or information was obtained. This means taking account of any sources used that are vulnerable to fraud and finding ways to be satisfied of their veracity. Where new technologies and innovative solutions are used, the TRA will be vital for the relevant person's ability to make determinations as to its reliability and independence.

Source documents, data or information must be current and valid to be of use in the CDD process. Where a document doesn't carry an expiry date, such as a utility bill or bank statement, it must be recently issued. Where it is a certified copy it must be recently certified as well as recently issued. Where documents must be signed by specific persons (for example auditors or reporting accountants) in order to be valid, relevant persons should obtain those signed documents (or appropriate copies of such) and not unsigned earlier drafts.

Other considerations in ensuring reliability and independence of source documents, data or information include:

3.3.4.1 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 should be aware of, and factor into their procedures, the limitations of documents used and what CDD information they actually verify. Relevant persons should also be conscious that some documents are more vulnerable to fraud than others. For those that are most susceptible to fraud, or where there is uncertainty concerning the veracity of the

document(s) presented, additional enquiries or other sources of information should be obtained to gain comfort. Relevant persons will need to be prepared to accept a range of documents and data.

3.3.4.2 Documents not in English

Relevant persons should ensure that documents obtained as part of the CDD process which are in a foreign language are adequately translated (independently from the customer) into English. This is to ensure the true significance of the document can be appreciated. Translation 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. If the decision is made not to translate a 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 signed off by a staff member of appropriate seniority. In cases such as this the relevant person must be able to demonstrate they have cumulatively taken appropriate steps to identify and verify the identity of the customer without these documents being translated.

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.

3.3.4.3 Photographs and signatures

In order to verify that the person you are dealing with is who they say they are, it will generally be necessary for identity verification documents to bear a photograph of the individual. Any photocopies showing photographs and signatures should be clearly legible. Either the relevant person itself, or the suitable certifier or introducer where used, should check that the photograph represents a good likeness of the customer and the document corresponds to the person whose identity is being verified.

3.3.4.4 Hard copy document verification and certification

Where CDD documentation is obtained in hard copy it can be vulnerable to forgery, particularly where the relevant person has not met the customer. To counteract this inherent vulnerability, certification that the document is a true copy of the original by a suitable certifier may aid relevant persons to establish the independence and reliability of the documentation. For this to have value in respect of identity documents, the certifier should have seen the original document in order to ensure the copy is genuine. The certifier should also have met the individual face to face in order to ensure any photograph of the customer is a good likeness and the document corresponds to the person whose identity is being verified.

Certification of documents by the relevant person itself is an option where the certifier is a member of staff who has met the person face to face. Otherwise, assessing the reliability and independence of certified copy source documents involves assessing both the certifier and the document itself. The results of the BRA and CRAs and the reliance to be placed on the certified documents will be primary considerations.

Code 4(1), (2)

The Authority has not prescribed a list of suitable certifiers. In applying a risk based approach, relevant persons should establish their own list of the types of certifiers they would consider suitable, bearing in mind the principles and considerations set out in this guidance. Such lists should be maintained and reviewed to ensure they continue to be appropriate taking into account the BRA, CRAs and TRA and any reviews of these risk assessments. Relevant persons must ensure they are satisfied on an ongoing basis that the certifier types listed in their procedures continue to enable them to manage and mitigate their ML/FT/PF risks.

For those relevant persons that may require further assistance, the Supplemental Information Document includes further information on certification of hard copy documents, including examples of suitable certifiers.

In respect of individual certifications, relevant persons will need to determine whether the individual on which reliance is placed as a certifier is suitable, in the context of that particular business relationship/occasional transaction, bearing in mind both the ML/FT/PF risk and reliance to be placed. Factors to consider may include the level of independence from the customer, when the certification took place, the certifier's stature, reputation and their track record with the relevant person, the relevant person's previous experience of accepting certifications from certifiers in that profession or jurisdiction, the adequacy of the AML/CFT/CPF framework in place in the jurisdiction in which the certifier is located and the extent to which the AML/CFT/CPF framework applies to the certifier.

Relevant persons will also need to ensure the certifier is clearly identifiable, contactable and accountable.

3.3.4.5 Use of electronic methods

The FATF has issued Guidance on Digital Identity, March 2020 which relevant persons may find useful in developing their own procedures and controls.

The Code and the Authority's guidance are technology neutral and so relevant persons may choose to use technology to meet their CDD obligations. The Authority does not endorse nor advise on specific methods or providers available to relevant persons.

Code 7

Technology used in the CDD process is ever-evolving and dynamic. Per the TRA, relevant persons must keep up to date with developments, including internationally, in this constantly changing field in order to ensure risks are

appropriately identified, assessed, and mitigated appropriately, so as to ensure ML/FT/PF risks are managed effectively and compliance with the Code.

Relevant persons should understand the basis for any electronic method, and be satisfied that it is sufficiently robust. This includes knowing what checks have been undertaken and the results of those checks. Relevant persons should also understand the method(s) used for corroboration of identity data and the potential for processes to be abused.

Code 33, 34, 35

Relevant persons should consider the capture, storage, accessibility and irretrievability of information and documentation used in the ID&V process and ensure that whatever methods are used can comply with the Code's record keeping, retention and format and retrieval requirements. Guidance regarding these requirements can be found at section 6.4.

Code 30(1)

Relevant persons must ensure that whatever electronic methods are used, they are capable of being monitored and tested to ensure they enable the relevant persons to meet their AML/CFT/CPF obligations as anticipated and continue to do so.

3.3.4.5.1 Terminology and concepts

There are many different types and uses of technology in the CDD process which a relevant person may choose to adopt. Some of the key terminology is summarised below.

- **Know Your Customer ("KYC") utility –** refers to a database which centralises the collection, verification, storage, and sharing of individuals' data and documents;
- **Electronic certification –** refers to the use of electronic apps / systems / programs to digitally certify documentation;
- **Electronic verification –** refers to the use of technology to verify in whole or in part the identity of an individual or entity; and
- **Independent electronic data source –** refers to a source of data collected or accumulated by an independent third party and available digitally.

Code 5, 7

KYC Utility

Some jurisdictions have developed, or are developing, KYC utilities. Systems similar to KYC utilities have also been developed by regulated firms who have collaborated to create shared access to digitised identity information and documentation.

Whilst there are no plans to introduce a national KYC utility on the Island at this stage, relevant persons should be aware that customers or potential customers may present with a digital identity where a KYC utility has been implemented in their resident jurisdiction. When considering a digital identity, relevant persons

should understand its basis and assess its suitability and reliability, alongside their risk appetite, CRAs and BRAs.

Electronic Certification

Developments in technology have meant that solutions are now available to relevant persons to digitally certify documentation. In order for a person to digitally certify a document, they must have seen the original document (as they would for a hard copy certification), in order to be able to declare that what they are certifying is a true copy of the original document. Relevant persons should satisfy themselves as to the reliability and veracity of the electronic certification method utilised to ensure it is not susceptible to manipulation.

Electronic Verification

Relevant persons may use technology to verify in whole or in part the identity of an individual or entity, which may be through the use of an app or electronic system.

Such apps / systems usually require the input of information / documentation by the end user, which is then automatically or manually checked and verified. Biometric data (such as 'selfie' videos or photographs) are often used for verification purposes by such providers.

Independent Electronic Data Sources

How an independent electronic data source can be used in the CDD process will depend on the depth, breadth and quality of the data used. In certain circumstances it may be possible to electronically verify a customer's identity and address, or it may be useful to verify that documents are authentic; but will not necessarily verify that a customer is who they say they are. Independent electronic data sources can provide a wide range of confirmatory material without involving a customer and are becoming increasingly accessible. An understanding of the depth, breadth and quality of the data accessed is important. Sources often used by electronic systems include: the passport issuing office; driving licence issuing authority; companies registry; the electoral roll; telephone directories; credit reference agencies; and other commercial / electronic databases.

Where a relevant person intends to use electronic data sources provided by commercial agencies, it should be sure that the agency is registered with a data protection agency in the UK or 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 consider:

- whether the source, scope and quality of the data is satisfactory.
- the number of matches of each component of an individual's identity or address that is appropriate 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.

3.3.4.5.2 Assessing and mitigating risks

The use of technology and electronic methods in the CDD process presents particular challenges and ML/FT/PF risks to relevant persons. It is important that relevant persons identify and assess any risks presented, and implement controls to mitigate them where appropriate. Guidance on assessing the ML/FT/PF risks associated with new technologies and the use of electronic methods for CDD purposes is at section 2.2.11.

The table below provides some examples of possible mitigation controls. This is not an exhaustive list.

Mitigation / Controls
Limiting the type of acceptable identity documents to those that contain: • high security features or biometric data such as finger prints and a facial image; • a qualified electronic signature created in line with national standards; • a feature that links the technology with trade registers or other reliable data sources such as companies registries; or • a feature that adjoins the technology with a government-established CDD data repository or a notified e-ID scheme, if the scheme's assurance level is sufficient.
Capture of documentation, and any photographs contained within that documentation, is of a high level of clarity and resolution, allowing for the contents to be enlarged to aid review.
Features built in to the technology to enable detection of fraudulent documents on the basis of documents' security features (e.g. watermarks, biographical data, photographs, lamination, and UV-sensitive ink lines) and the location of various elements in the documents (i.e. optical character recognition).
Image of documentation captured is automatically examined to confirm the existence of certain security features, such as holograms or watermarks.
Image of documentation captured is matched to a 'template' of the particular type of identity document presented to compare the security features ingrained in the ID document presented.
Data contained in a document is compared to biometric / other stored data on the machine readable code (MRZ code) or other algorithm within the document.

Data contained in a document is automatically examined for the use of unauthorised print fonts or character spacing.
Image of documentation captured is manually examined by individual(s) specifically trained to detect tampering or forgery, or to spot situations where the person on a screen looks different from the person on the identity document.
The app / system / programme uses controls in the copying of the document, photography, and transmission process, providing no opportunity to tamper with or manipulate the documents or photographs provided.
Use of a highly secure connection for transmission.
Security of the app / system / programme is regularly tested in order to guard against hacking or security breaches.
Use of a "selfie" which is biometrically compared / matched to photographic identity documentation provided.
Use of a video or "micro-stream" of photographs to capture facial movements to confirm the individual is present at the time the photograph is taken.
Use of a live chat with an administrator with specialist training in how to identify possible suspicious or unusual behaviour or image inconsistencies.
Use of a code or password sent to the user, who then provides a photograph displaying the code or password, immediately before photographing and uploading the relevant identity documentation, to confirm the individual is present at the time photograph is taken
Use of location matching to determine whether the information / documentation / photographs are captured is consistent with the user's place or country of residence
Use of anti-impersonation measures such as requiring the user to verbally repeat word or phrases as dictated by the relevant person during a video call
Built in computer applications that automatically identifies and verifies a person from a digital image or a video source (e.g. biometric facial recognition).
Built in security feature that can detect images that are or have been tampered with (e.g. facial morphing), whereby such images appear pixelated or blurred.
Require screen to be adequately illuminated when taking a person's photo/recording a video during the CDD process.

3.3.5 Financial inclusion when usual documentation cannot be provided

The FATF has issued Guidance on financial inclusion which relevant persons may find useful in developing their own procedures and controls:

- February 2013 – Revised Guidance on AML/CFT and Financial Inclusion
- November 2017 – FATF Guidance on AML/CFT Measures and Financial Inclusion
- The FATF's Guidance on Digital Identity, March 2020 also provides useful information on financial inclusion.

Some customers may not be able to provide all aspects of identity information or documentation, or the relevant person may not be able to undertake the suggested additional checks. This does not automatically equate to low or lower ML/FT/PF risk. It is one factor in a holistic assessment. Financial exclusion can

affect both individuals and businesses and have many reasons. For individuals this can include a poor credit rating or a criminal background. Institutions should not therefore apply simplified CDD or exemptions solely on the basis that the customer is financially excluded.

Code 4(2) Where a relevant person's normal procedures are not followed in respect of particular cases they must be mindful of the requirement to ensure their procedures and controls enable them to manage and mitigate their ML/FT/PF risks.

Relevant persons should adopt a case-by-case approach in understanding why a customer is unable to provide the relevant information or verification and in determining what methods they will accept to verify the customer's identity and/or address. The relevant person must be satisfied as to the validity and veracity of any documents accepted. The relevant person should have procedures in place to clearly document why they have been unable to verify the customer's identity and/or address using their typical methods, what measures they have taken to verify their customer's information and why they feel that this is sufficient to satisfy the requirements of the Code including how it manages and mitigates their ML/FT/PF risk. Including, within their procedures, a requirement for Senior Management consideration and sign off for such exceptions before the relationship/transaction is allowed to progress, may assist relevant persons to achieve this balance.

Relevant persons should also be mindful that alternative forms of identity verification may be more susceptible to fraud and abuse and take appropriate measures to mitigate that risk effectively. Such measures would including enhanced monitoring of the business relationship or providing access only to certain lower risk products and services.

3.3.6 Change of CDD information

Code 4(2), 10(3), 13(1) Where CDD information in relation to a customer changes, relevant persons must conduct CDD procedures relevant to the change(s) taking a risk based approach (including consideration of what the change is).

This would include changes to specific pieces of identity information previously obtained such as a change in name or address.

Code 12, 8, 10, 11 This principle also applies 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 or control of a customer or in respect of other persons specified at paragraph 12 of the Code. In such cases, relevant persons must treat these persons as new relationships and paragraph 12 CDD requirements must be applied as required by paragraphs 8 and 11 of the Code. For example, where a director of a company or a council member of a foundation is replaced, the procedures required under paragraph 12 of the Code must be followed. In line with the timing requirements for conducting CDD, these procedures must be completed before the new person

is allowed to exercise control over the customer's business relationship with the relevant person.

Code 6(2) Consideration should also be given as to whether the change of CDD information may impact on the CRA.

Code 13(1) In addition, changes of CDD information should prompt consideration as to whether the relationship and CDD information should be reviewed more extensively.

Guidance on ongoing CDD/ECDD monitoring is at section 3.4.6.

3.3.7 Bearer shares

Many jurisdictions, including the Isle of Man, have prohibited or immobilised bearer shares due to the associated AML/CFT/CPF 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.

3.3.8 Sanctions

Code 4(1)(a), 13(1)(c) Relevant persons should check a customer's (including beneficial owner's and controller's where appropriate) nationality, residency, expected activities and source of funds to ensure that they are not subject to any relevant financial sanctions both at the outset of the relationship and also on an ongoing basis. More information on sanctions can be found in guidance published by ~~IOMCE~~IOMCI.

3.3.9 Reporting suspicions

Code 3(1), 26 Where a relevant person identifies any suspicious activity, an internal disclosure must be made. This is required for both existing and prospective customers, including where a business relationship with a prospective customer has not proceeded. The requirement is irrespective of the type of prospective customer. Guidance on making internal disclosures is at section 5.4.

3.4 Code CDD requirements

3.4.1 Minimum standards table

The following table provides a 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 Handbook.

	Lower and Standard Risk (CDD) (Code paras 8, 11, 12, 13)	**Higher Risk (CDD and ECDD~~)(EDD~~)** (Code para 15)	**Foreign PEPs & Higher Risk Domestic PEPs** (Code para 14 and 15 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 assessment.
Verification of that information (Customer)	Generally required before or during the formation of the relationship, but in **very limited circumstances** may be undertaken following the establishment of the business relationship		
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 generally required before or during the formation of the relationship, but in **very limited circumstances** may be undertaken following the establishment of the business relationship		
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

3.4.2 New business relationships and occasional transactions

Code 8(1), 11(1)

8 New business relationships / 11 Occasional transactions
(1) A relevant person must, in relation to each new business relationship / an occasional transaction, establish, record, maintain and operate the procedures and controls specified in sub-paragraph (3).

Code 8(3), 11(3), 15

8 New business relationships / 11 Occasional transactions
(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 / occasional transaction; and

(e) take 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(s) 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

Code 8(3), 10, 12

Due to the similarity of requirements at paragraph 8(3) with those of other Code paragraphs (such as paragraphs 10 and 12), detailed guidance on each of the requirements 8(3)(a) to (e) is as follows:

- Identifying the customer – see section 3.5;
- Verifying identity and legal status – see section 3.6;
- Nature and intended purpose of the business relationship – see section 3.7; and
- Source of funds – see section 3.8.

Code 14, 15

For higher risk customers, additional procedures may be needed. Guidance on ECDD is at section 3.4.7 and guidance on customers where there are PEPs is at section 3.8.8.

Code 3(1), 11(4), 11(5)

Section 4.1 provides details of "exempted occasional transactions" to which certain requirements of Code paragraph 11 may not apply in certain circumstances.

Code 8(2), (4), 11(2)

The timing for when these procedures must be undertaken, including exceptions, is set out in the Code, see section 3.4.8.

3.4.3 Introduced business

Code 9(1), (2), 8, 11

9 Introduced business

(1) This paragraph applies where a customer is introduced to a relevant person by a person who provides elements of the customer due diligence (the **"introducer"**).

(2) The relevant person must comply with –

(a) this paragraph; and

(b) paragraph 8 or 11 (whichever is applicable).

Where paragraph 9 of the Code applies, this is referred to as "introduced business". Paragraph 9 was required to have been followed for all new customers by May 2020. For existing customers paragraph 9 may be deferred until there is a trigger event, or when the CRA is reviewed (see sections 2.2.9 and 2.2.6).

Code 9, 8, 10, 11, 12, 13 14, 16, 17, 18, 19, 20, 21, 22, 36, 37, 39

Paragraph 9 refers to "elements of customer due diligence" which are provided to the relevant person during the establishment of a business relationship, by a person (a third party, known as an introducer) who is not the customer. The introduction stage refers to any time prior to the business relationship start date. This includes the different aspects of all the CDD measures specified in paragraphs 8 to 14, 16 to 22, 36, 37 and 39 of the Code. For example:

- identifying the customer;
- verifying a customer's identity;
- verifying the legal status of a customer;
- identifying a beneficial owner;
- verifying a beneficial owner's identity;
- obtaining information on the nature and intended purpose of the business relationship; and
- taking measures to establish the source of funds.

Code 9

If any of the above elements are provided to the relevant person by a third party (an introducer), paragraph 9 applies. Elements of CDD may be received from more than one source or introducer during the establishment of the business relationship.

Paragraph 9 also refers to "evidence of verification of identity". Evidence of verification of identity is a much narrower element of CDD and simply means the use of reliable, independent source documents, data or information to verify the identity of the customer or beneficial owner of the customer. Where evidence of identity is provided to a relevant person by an introducer (or another third party if permitted by the Code) any document(s) provided should be in accordance with the relevant persons' policies and procedures.

Code 4(3)

Where paragraph 9 applies, the relevant person retains the ultimate responsibility for ensuring that CDD complies with the Code.

3.4.3.1 What is introduced business?

An introducer includes any third party(ies), who is not the customer, that is involved in the provision of CDD to the relevant person, whether or not that third party is bringing the customer to the relevant person in a broader introductory sense. This can include, but is not limited to;

- A financial adviser (whether in the Island or elsewhere): for example establishing an investment relationship for a customer with an investment management firm or life insurer in the Island (relevant person), where the adviser provides elements of the CDD to the investment manager / life insurer;
- A lawyer or accountant (individual or firm, whether in the Island or elsewhere): for example introducing / bringing a customer to a TCSP in the Island (relevant person) for the purpose of establishing / transferring a structure, where the lawyer (including a family office) provides elements of the CDD in respect of the customer;
- A TCSP (whether in the Island or elsewhere): for example establishing a banking relationship for a client company with a bank in the Island (relevant person), where the TCSP provides elements of the CDD in respect of the client company;
- Any other employee(s) of a third party or non-trusted persons engaged to act on behalf of a beneficial owner(s).

3.4.3.2 What is not introduced business?

Below are some examples of what is not introduced business. A diagram is also provided to assist in assessing whether there is an introduced business relationship for the purpose of the Code.

Referrals

Introduced business (for the purpose of the Code) is not the same as a referral. In the AML/CFT/CPF context, a referral is limited to, for example, where a third party informs a prospective customer to go to a particular relevant person and the third party does not provide any CDD to the relevant person, other than the name and contact details of the prospective customer.

Circumstances where a third party is providing solely the name and contact details of the underlying customer to the relevant person do not fall within the definition of introduced business.

Suitable certifiers

Introduced business is not the same as providing a suitable certification. Suitable certifiers are provided with the original CDD documentation by the prospective customer who they have met. The suitable certifier certifies hard copies of those documents and returns them to the customer who provides them to the relevant person.

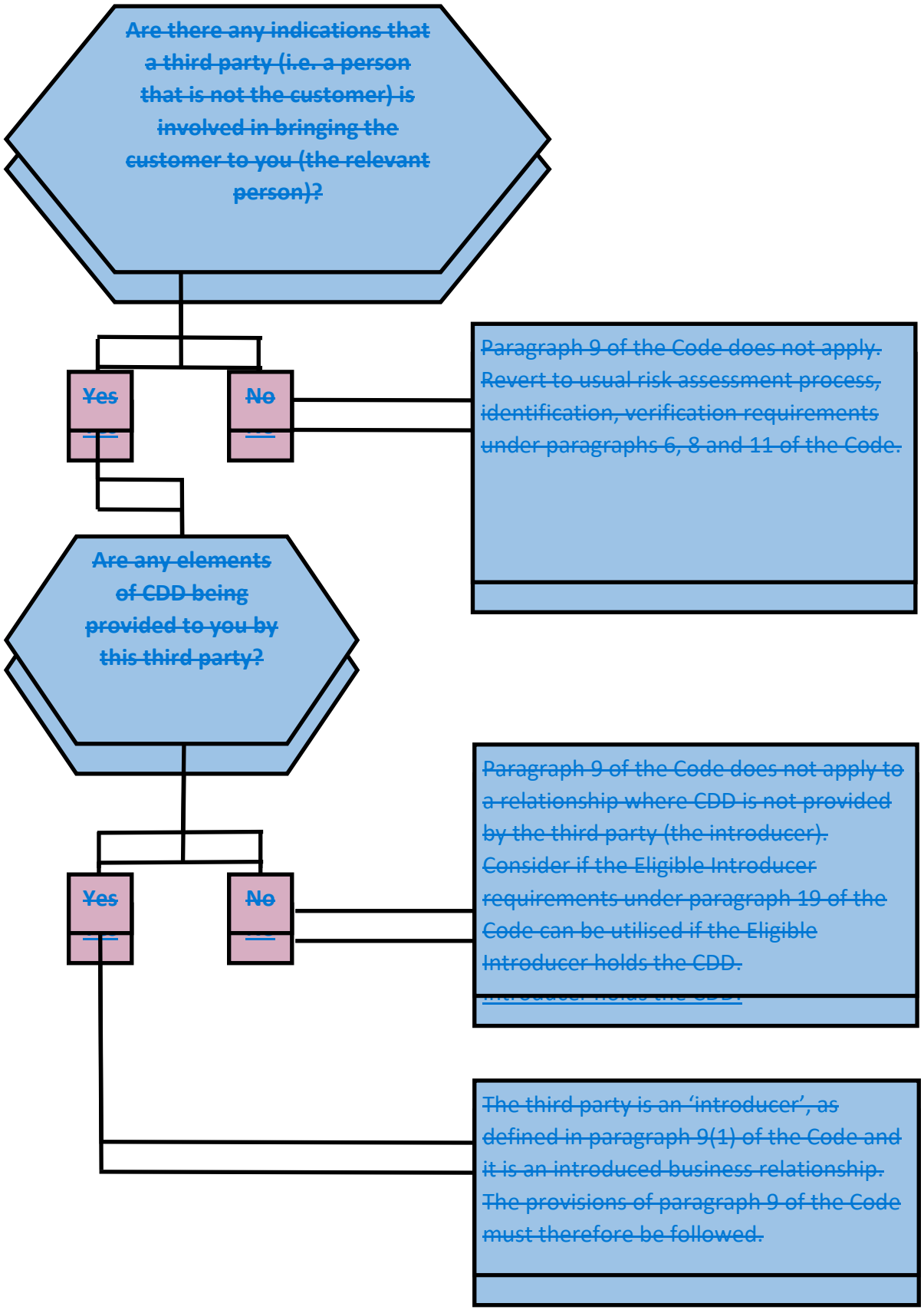
Code 9, 19

Eligibly introduced business

Introduced business under paragraph 9 of the Code is different from eligibly introduced business under paragraph 19 of the Code. Under paragraph 9 the relevant person taking on the introduced customer must have all the necessary CDD information and verification for the prospective customer at the outset of the business relationship/occasional transaction. The only reliance that may be placed on a paragraph 9 introducer is as a conduit for elements of CDD information/verification.

For eligibly introduced business the relevant person can rely on the eligible introducer to hold evidence of customer identity on its behalf (subject to the paragraph 19 conditions). Information about eligibly introduced business can be found at 4.5.

Determining if there is an introduced business relationship



3.4.3.3 Introduced business requirements

Code 9

Paragraph 9 provides specific additional requirements for introduced business and emphasises ECDD requirements should the broader CRA indicate higher ML/FT/PF risk.

Code 9(3), (4)

Broader Customer Risk Assessment – the Introducer Risk Assessment

A risk assessment of the introducer is required as an add-on to the CRA. This is to address the potentially increased ML/FT/PF risk of accepting customers introduced by a third party (introducer) that provides elements of their CDD. Guidance on the introducer risk assessment, specified considerations pertaining to third parties and how these integrate with the CRA can be found at section 2.2.10.

ECDD

Code 9(5)

9 Introduced business

(5) If the risk assessment indicates higher risk, the relevant person must undertake enhanced customer due diligence on the customer in accordance with paragraph 15 including, taking reasonable measures to establish the source of wealth of the customer and any beneficial owner of the customer.

Code 9(4), (5), 15 (2), (3)

Paragraph 9(5) of the Code emphasises and reiterates paragraph 15(3) in that if a CRA, which includes the introducer risk assessment and other matters specified at paragraph 9(4), indicates a higher ML/FT/PF risk, the relevant person must undertake ECDD as outlined at paragraph 15(2) of the Code. Paragraph 9(5) also reiterates one aspect of ECDD listed at 15(2)(c), that of taking reasonable measures to establish the source of wealth.

Guidance on undertaking ECDD is at section 3.4.7, guidance on the particular ECDD requirement to establish source of wealth is at section 3.8.5.

Third party location

Code 9(6), (4), (7)

9 Introduced business

(6) If more than one third party located outside of the Island is involved in the process, as specified in sub-paragraph (4), sub-paragraph (7) applies.

This sub-paragraph only applies where there is more than one third party involved in the process of transmitting CDD to the relevant person, and these third parties are located outside of the Island. It is possible that any number of such third parties may be interposed between the third party that actually meets the customer and the party that acts as introducer to the relevant person. Therefore, information and evidence could be passed through a number of layers before it finally arrives at the relevant person, through the introducer. Strictly speaking each third party acts as an "introducer" to the next, but in this part of the guidance we use the term "introducer" for that third party which introduces the customer to the relevant person in the Island, and the term "third party" is used for all others.

Code 9(6), (7)

Where any such third parties involved in the process are located outside the Isle of Man this may have a negative impact on the CRA carried out under paragraph 6 of the Code. This is because such third parties will not be overseen or regulated by the Authority, therefore the Authority will not be as fully informed about their integrity or competence as it would be about an Isle of Man regulated or overseen business. For this reason it is possible that the CDD information and evidence of identity received from, or through, such third parties may not be as accurate or complete as would normally be required. Whether those third parties are trusted persons or not has no impact on the requirements of sub paragraphs 9(6) and 9(7).

Code 9(7)

As the involvement of more than one third party outside the Island in the process poses an increased risk that the evidence of verification of identity obtained by the relevant person from the introducer may not be reliable, additional safeguards and requirements are in place, as set out below. In these circumstances such evidence of verification of identity must be obtained more directly by the relevant person, using one of the options set out in sub-paragraph 9(7).

Code 9(6)

It should be noted that a party (located outside the Island) who directly introduces a customer to a relevant person in the Island will be an introducer and will not therefore count as a third party outside the Island. If, however, the relevant person in the Island (*relevant person A*) introduces that customer to a further relevant person in the Island (*relevant person B*), then for relevant person B the party located outside the Island will constitute a "third party outside the Island" for the purposes of sub-paragraph 9(6).

Code 9(6), 6(4)

For the avoidance of doubt, the number of parties involved in any "chain" within the Island does not impact on sub-paragraph 9(6), but must be considered when undertaking the CRA required under sub-paragraph (4) and paragraph 6 of the Code. Guidance regarding CRAs can be found at section 2.2.9.

Verification of identity and meeting the customer

Code 9(7)

9 Introduced business

(7) The relevant person must verify the identity of the customer using reliable, independent source documents, data or information obtained, either —

(a) directly from the customer; or

(b) from the introducer, but only if the introducer has obtained such evidence of verification of identity —

(i) directly from the customer; or

(ii) directly from a third party who has met the customer; or

(c) directly from a third party who has met the customer.

If it is identified there is more than one third party involved in the process of transmitting CDD to the relevant person and these third parties are located outside of the Island, the steps set out in sub-paragraph (7) are mandatory.

The requirements in this sub-paragraph are only in respect of evidence of verification of identity, not in respect of other CDD information (although the relevant person may choose to obtain other CDD information using this route). This is because identification (and therefore evidence of verification of identity) of the customer is the single most important piece of CDD. It is therefore of upmost importance that evidence of verification of identity be of the highest standard that can practically be obtained.

The requirement of the paragraph is that:

The relevant person must verify the identity of the customer using reliable, independent source documents, data or information. This is the standard requirement for verification of identity prescribed by the Code.

Code 4(2), 5, 6, 7, 9(7)

The acceptability of a third party's involvement in providing evidence of verification of identity at 9(7) is conditional on whether that third party has met the customer. Meeting a customer may mean the customer was physically present with the third party. However, in the digital age, being physically present is not necessarily the only method of meeting a customer. Whether the relevant person considers it appropriate to use other methods and what other methods they consider appropriate in any particular instances or cases will depend on the outcomes from their BRA, TRA and CRAs (including the introducer risk assessment and third--party considerations).

Where third parties are involved, the relevant person will need to understand what "meeting the customer" means to that third party and whether the processes and procedures they have followed in any particular case satisfy the relevant person's own policies and procedures for meeting a customer.

Code 4(2)

Relevant persons must be mindful of the overarching obligation that their procedures and controls must enable them to manage and mitigate their ML/FT/PF risks.

Guidance on verifying the identity of a customer etc. can be found at section 3.6. The Supplemental Information Document provides further information about verification of identity including an example method for meeting a customer using innovative technology for relevant persons needing further assistance.

The options are as follows:

(a) Directly from the customer

This may provide the relevant person with a higher level of certainty about the identity of the customer than the other options in sub-paragraph (7) as no third parties are involved in the transmission process.

(b) From the introducer

The relevant person may still obtain the evidence of verification of identity directly from the introducer, i.e. the third party that directly introduces the customer to the relevant person. This is only acceptable if the introducer has obtained it:

(i) directly from the customer

The same comments apply here as where the relevant person obtains the material directly from the customer, but the degree of certainty about the identity of the customer may be lower as an additional party is now interposed between the customer and the relevant person in the transmission process; or

(i) directly from a third party who has met the customer

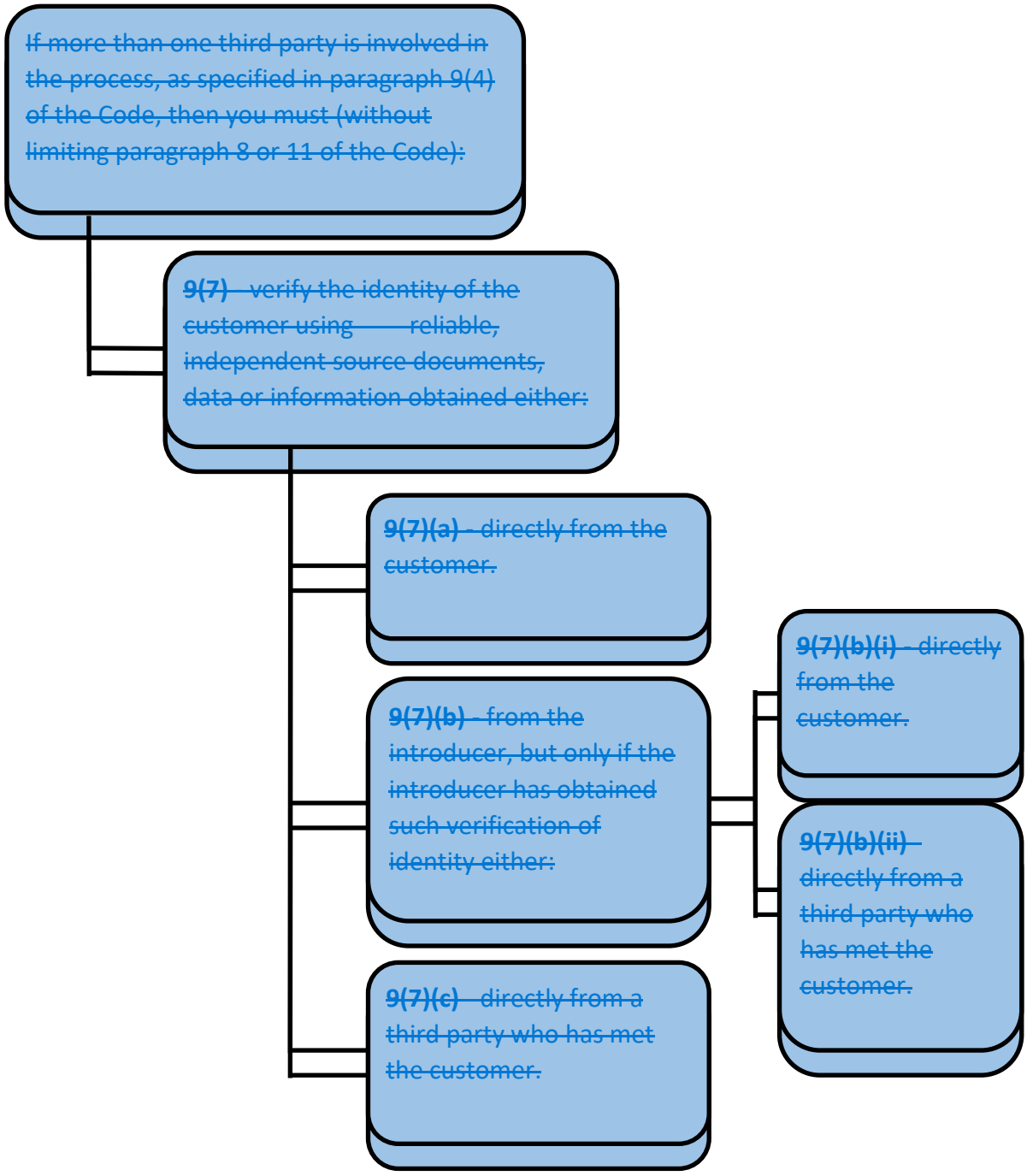
This option would cover the scenario where the introducer obtains the evidence of verification of identity directly from the third party who originally met the customer and initiated the introduction process that ultimately resulted in the introduction to the relevant person. Here, the introducer would go back and obtain the material from the "first link in the chain" therefore reducing the number of third parties interposed between the customer and the relevant person.

The option would also cover the scenario where the introducer approaches an entirely different third party with links to the customer who may have played no part in the introduction process (for example the customer's lawyer). The only requirement is that the third party concerned has met the customer and the evidence is obtained directly.

(c) directly from a third party who has met the customer

This option would cover the scenario where the relevant person obtains the evidence of verification of identity directly from the third party who originally met the customer and initiated the introduction process that ultimately resulted in the introduction to the relevant person. Here, the relevant person would go back and obtain the material from the "first link in the chain" therefore reducing the number of third parties interposed between the customer and the relevant person.

A flow diagram relating to the verification requirements where more than one third party is located outside of the Island can be found below.



Code 9

Due to the complexity of the requirements at paragraph 9, a number of example scenarios are provided in the Supplemental Information Document showing how 9(6) and 9(7) should be interpreted in practice. Whilst these scenarios have been written using specific sectors, the circumstances described are applicable to all sectors.

(d) A third party

Code 9(10)

9 Introduced business

(10) For the purposes of this paragraph, a third party "involved in the process" does not include a third party in the same group as-

(a) the relevant person; or

(b) the introducer,

provided that third party is a trusted person.

Code 3(1)

3 Interpretation

(1) In this Code -

"group", in relation to a body corporate ("B"), means —

(a) B;

(b) any other body corporate that is B's holding company ("H") or B's subsidiary; and

(c) any other body corporate that is a subsidiary of H,

and **"subsidiary"** and **"holding company"** shall be construed in accordance with section 1 of the Companies Act 1974 or section 220 of the Companies Act 2006 (as applicable);

This means that any company that is a party in a chain of parties involved in the transfer of CDD information and evidence of verification of identity to the introducer, or the relevant person, which is a subsidiary or a subsidiary of the same parent company of the introducer or relevant person, should not be included in the calculation of the number of third parties involved in the process outside the Island. However, for such a company to be "discounted", it must be a trusted person as defined in the Code as-

Code 3(1)

Interpretation

(1) In this Code -

"trusted person" means -

(a) a regulated person;

(b) a nominee company owned by a regulated person, where the regulated person is responsible for the nominee company's compliance with the AML/CFT legislation;

(c) an advocate within the meaning of the Advocates Act 1976 or a registered legal practitioner within the meaning of the Legal Practitioners Registration Act 1986 and who is registered as a designated business for those activities;

(d) an accountant who is registered as a designated business for this activity;

(e) a person who acts in the course of external regulated business; or

a nominee company owned by a person who acts in the course of external regulated business where that person is responsible for the nominee company's compliance with AML/CFT requirements at least equivalent to those in this Code.

Note that the Code provides definitions at 3(1) for a number of the other terms used in the quoted extracts above.

Code 9(6)

For the avoidance of doubt, this provision only applies to those corporate entities that fall within the above definition. If third party companies involved in the process simply have the same beneficial owners as the introducer or relevant person but are not structured as a corporate group, then they should be considered as quite separate individual companies for the purposes of sub-paragraph 9(6).

Code 9(10)

An example scenario showing how paragraph 9(10) should be interpreted in practice is in the Supplemental Information Document.

Other provisions

Code 9(8)

9 Introduced business

(8) The relevant person must be satisfied that –

(a) any element of customer due diligence information provided by the introducer conform to the requirements of this Code;

(b) any document, data or information used to verify the identity of the customer conform to the requirements of this Code; and

(c) there is no reason to doubt the veracity of the document, data or information produced to verify the identity of the customer.

Code 9(11), (7), (4), 6

9 Introduced business

(11) For the avoidance of doubt, if further elements of customer due diligence other than evidence of verification of identity are obtained by the relevant person under sub-paragraph (7) then this should be reflected in the customer risk assessment carried out in accordance with paragraph 6 and sub-paragraph (4).

Code 9(4), (7), 6

This sub-paragraph provides that if the relevant person in the Island is required by sub-paragraph 9(7) to go directly to the customer, or a third party who has met the customer to obtain evidence of verification of identity, it may, if it so decides, obtain some or all of the other CDD using this route. This may have the effect of

mitigating the CRA carried out for the purposes of sub-paragraph 9(4) and paragraph 6 of the Code. The number of third parties involved in the process would be reduced to a maximum of one and the only third party involved (if any) would have met the customer.

3.4.4 Continuing business relationships

Code 10, 8

10 Continuing business relationships

(1) A relevant person must, in relation to each continuing business relationship, establish, record, maintain and operate the procedures and controls specified in sub-paragraph (3).

(2) The procedures and controls must be undertaken during a business relationship as soon as reasonably practicable.

(3) Those procedures and controls are –

(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. It also includes any business relationships held prior to AML/CFT/CPF requirements coming in for a particular business sector. It is anticipated this will only affect a small number of relevant persons.

Code 10(3)

If verification of identity has not already been obtained, or that which was obtained is unsatisfactory (for example, because the verification requirements have been enhanced since the original verification of identity was obtained or the assessed risk of the relationship has changed), relevant persons must take steps to obtain satisfactory verification of identity. Where verification of identity documentation obtained previously has subsequently expired (e.g. a passport expiring a relevant person does not automatically have to update this documentation.

Code 13(1)

Paragraph 13 of the Code sets out ongoing monitoring requirements for customers where satisfactory CDD was undertaken at the outset of the business relationship or transaction (see section 3.4.6). For these continuing relationships, whether CDD needs to be undertaken will depend upon whether the relevant person has already

obtained the relevant information and documentation and whether, if it has been obtained, it is satisfactory and complies with current standards.

Code 10

Relevant persons will therefore need to examine the information and documentation already held to determine whether it is necessary to collect additional CDD or make further enquiries either from the customer 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 accurate and/or appropriate, the procedures under paragraph 10 of the Code should be used.

3.4.5 Beneficial ownership and control

Code 12(1), Parts 3, 4, 5, 6

This part of the document explains the CDD requirements for the natural persons associated with different types of customer. These requirements are relevant when operating the procedures and controls required in Parts 3-6 of the Code.

The Code's definition of beneficial owner differs from definitions in the Beneficial Ownership Act 2017. The Authority has issued guidance regarding the Beneficial Ownership Act 2017, which can be found here. Additionally, relevant persons should be aware that other pieces of legislation contain definitions regarding "control" which they may be required to incorporate into their procedures.

Code 3(1)

3 Interpretation

(1) In this Code -

"Beneficial owner" means a 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;

Code 3(1), 12(2)(a)

A relevant person must be satisfied it knows who the beneficial owner of its customer is, down to the natural person(s) that ultimately owns or exercises ultimate effective control or significant influence over the customer, and/or on

whose behalf a transaction or activity is being conducted. This must be done irrespective of the number of persons or arrangements of any description necessary to go through to reach that natural person(s).

Relevant persons should be aware that control over a customer can include:

- control without direct ownership, for example through close family relationships, or historical or contractual associations;
- using, enjoying or benefiting from the assets owned by the customer; and
- responsibility for strategic decisions that fundamentally affect the business practices or general direction of a legal person.

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 using any simplified CDD measures for the customer and any associated persons as explained in chapter 4.

Code 12(2)

Paragraph 12(2) of the Code deals with the inherent differences in beneficial ownership where customers are non-natural persons versus customers that are natural persons.

Where the customer is a non-natural person such as a company or a legal arrangement, beneficial ownership has a broader scope. Ownership or control of the legal person or arrangement is a factor as well as determining whether that customer is acting on behalf of someone else i.e. on whose behalf a transaction or activity is conducted.

Where a customer is a natural person, beneficial ownership is narrower in scope as it is not possible to legally own a natural person. Beneficial ownership involves determining whether that customer is acting on behalf of someone else i.e. on whose behalf a transaction or activity is conducted.

Code 12(2)(c)

Paragraph 12(2) also brings a further concept, which whilst not strictly one of beneficial ownership, is relevant to issues of control as it requires determining whether a person(s) is acting on behalf of a customer (of any type) in an authorised capacity.

These nuances of beneficial ownership as applicable to different types of customer are set out below.

Code 12(2)(a), 11(4), (5), 16(2), 18(2)

Paragraph 12(2)(a) of the Code is only relevant where a customer is not a natural person.

12 Beneficial ownership and control
(2) Relevant persons must, in the case of any customer –

(a) which is not a natural person -

> (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;

Code 12(2)(b), 17, 21

Paragraph 12(2)(b) of the Code is relevant for all customers, natural and non-natural alike.

> **12 Beneficial ownership and control**
> (2) Relevant persons must, in the case of any customer –
>
> (b) 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;

When determining if a customer is acting on behalf of another person (for the purpose of this guidance "an underlying client") an important consideration is the nature of the relationship between the relevant person, the customer and the underlying client (where one may exist), and how control over the relationship is exercised (by the customer or the underlying client). Determining control in relation to a business relationship should be considered by the relevant person on a case-by-case basis.

Code 12(2)(b)

Factors that may indicate an underlying client is controlling the relationship with the relevant person, and therefore that the customer may be acting on behalf of that underlying client, per 12(2)(b) of the Code, include:

- instructions frequently being made directly by the underlying client which are then implemented by the customer on the underlying client's behalf;
- the underlying client has signatory rights over the relationship with the relevant person;
- the immediate source of funding of the business relationship is identified as coming directly from the underlying client, rather than from the customer;
- funds are remitted directly back to the underlying client rather than to the customer.

If uncertainty remains regarding who is controlling the business relationship with the relevant person, other factors to consider that may indicate the customer is acting on behalf of an underlying client include:

- whether the account title indicates there could be an underlying client;
- whether there are payment or transaction references, or rationale for payment / transactions, that do not appear to relate to the purported customer, or that could indicate there is an underlying client exercising control;
- whether it appears that the customer has had to refer to an underlying client to obtain information; and
- what is covered by the terms of business entered into with the customer.

Code 12, 17, 21

If the relevant person's assessment of the business relationship indicates that the customer is acting on behalf of an underlying client, in addition to identifying and verifying the customer the relevant person must also identify, and verify the identity of, the underlying client. This is subject to certain simplified CDD concessions at paragraphs 17 and 21 of the Code, which remove the requirement on the relevant person at 12(2)(b) to identify and verify the identity of the underlying client provided relevant conditions are met. Note that all other requirements under paragraph 12 still apply. Guidance on paragraphs 17 and 21 can be found at 4.3 and 4.7.

Code part 4

If a relevant person determines that there is no underlying client (which in many cases will be obvious and straightforward) 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 their customer is, whether they are acting for another person, and if so what CDD is required.

Code 12(2)(c)

Paragraph 12(2)(c) of the Code is also relevant for all customers, natural and non-natural alike.

12 Beneficial ownership and control

(2) Relevant persons must, in the case of any customer –

(c) determine whether a person is acting on behalf of a customer and verify that any person purporting to act on behalf of the customer is authorised to do so; and, if so —

(i) identify that other person; and

(ii) take reasonable measures to verify the identity of that person using reliable, independent source documents, data or information.

Paragraph 12(2)(c) is intended to ensure that any persons (whether natural or otherwise) acting on behalf of a customer of any type have the correct authority to do so. It is important that relevant persons understand and document the

rationale for such arrangements and are comfortable with them from an AML/CFT/CPF perspective.

If there is such a person(s), identity information must be obtained and reasonable measures to verify their identity undertaken. Persons acting on behalf of a customer would include a customer appointing another person as an account signatory e.g. an expatriate appointing a member of their family, or company directors appointing a non-director as a signatory, or granting power of attorney in favour of a third party.

Code 12(2) – 12(10)

The requirements at 12(2) are expanded (and not in any way limited) at paragraphs 12(3) to 12(10) for specific types of non-natural person or product. As a result, the guidance for paragraphs 12(3) to 12(10) of the Code must not be considered in isolation. They must be considered in conjunction with the guidance on paragraph 12(2) of the Code and with each other as appropriate.

3.4.5.1 Legal arrangements

Additional requirements are in effect for customers that are legal arrangements.

Code 12(3)

12 Beneficial ownership and control

(3) Without limiting sub-paragraph (2) a relevant person must, in the case of a legal arrangement, 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.

Code 12(2), (3)

This means identifying and verifying the identity of the natural persons that ultimately fulfil these roles through any number of persons or arrangements of any description and includes, 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 and verify the identity of the individual who gave the instructions to form the legal arrangement and any person funding the establishment of the arrangement.

Obtaining information about classes of beneficiaries enables relevant persons to have the capacity to determine the identity of a beneficiary in future and appropriately risk assess the relationship.

3.4.5.2 Foundations

Additional requirements are in effect for customers that are foundations.

Code 12(4)

12 Beneficial ownership and control

(4) Without limiting sub-paragraph (2) a relevant person must, in the case of a foundation, 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.

Code 12(4)(c)

In respect of 12(4)(c), obtaining information about classes of beneficiaries enables relevant persons to have the capacity to determine the beneficiary in the future and appropriately risk assess the relationship.

Code 12(4)(e) Foundations Act 2011

In respect of 12(4)(e), an example of a person exercising ultimate effective control includes "a person with sufficient interest" as defined in the Foundations Act 2011 (or equivalent in non-Isle of Man established foundations).

3.4.5.3 Legal Persons (including foundations)

Additional requirements are in effect for customers that are legal persons (including foundations).

Code 12(5), (2), (4)

12 Beneficial ownership and control

(5) Without limiting sub-paragraphs (2) and (4), in respect of a customer that is a legal person, the 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.

Code 12(5)(a), (b)

This means identifying and taking reasonable measures to verify the identity of the natural person(s) that ultimately own or control the legal person. Relevant persons should make every effort to identify who such natural person(s) is/are.

Code 12(5)

Relevant persons should only resort to identifying the natural person(s) specified at 12(5)(c) of the Code where it is not possible to comply with the requirements at 12(5)(a) and (b) of the Code. In determining that complying 12(5)(c) of the Code is the only option, relevant persons should:

- ensure that they have exhausted all possible means for identifying the natural person(s) at 12(5)(a) / (b) of the Code;
- be satisfied that their inability to identify the natural person(s) at 12(5)(a) /(b) does not give rise to ML/FT/PF suspicions; and
- ensure they are satisfied that the reason given by the customer as to why the natural person(s) per 12(5)(a)/(b) cannot be identified is plausible.

When deciding which natural person(s) under 12(5)(c) of the Code to identify and verify identity as the beneficial owner, relevant persons should consider who has the ultimate and overall responsibility for the customer and can take binding decisions on the customer's behalf.

The rationale and steps taken must be clearly documented by the relevant person in accordance with the record keeping requirements.

3.4.5.4 Legal persons (including foundations) and Arrangements

Additional requirements are in effect for customers that are legal persons (including foundations) or legal arrangements.

Code 12(6)(a), 12(2) - (5)

12 Beneficial ownership and control

(6) Without limiting sub-paragraphs (2) to (5), in the case of a customer that is a legal person or a legal arrangement the relevant person must –

(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 refers to persons exercising control over the management and having power to direct the activities of a customer that may not be deemed to be a controller, or one of the parties referred to above. This includes signatories, directors/council members as well as persons with powers of attorney.

Code 3(1)

For legal persons not listed on a recognised stock exchange, this also 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 or significant influence 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 legal arrangements, this includes the trustee or other person who exercises ultimate effective control or significant influence over the legal arrangement. Such as, the 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.

Code 12(6)(b), 12(2) - (5)

12 Beneficial ownership and control

(6) Without limiting sub-paragraphs (2) to (5), in the case of a customer that is a legal person or a legal arrangement the relevant person must –

(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

Code 4(2)

This includes obtaining information about the identity of such persons and their roles and powers. It includes obtaining copies of authority such as Memoranda and Articles of Associations, Power of Attorney, a signatory list plus a copy of a board resolution relating to the signatory list. Relevant persons must take a risk based approach and (where not otherwise required by the Code) 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.

Code 12(6)(c), 12(2) - (5)

12 Beneficial ownership and control

(6) Without limiting sub-paragraphs (2) to (5), in the case of a customer that is a legal person or a legal arrangement the relevant person must –

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

Code 6

Understanding the nature of the customer's business includes understanding what business the customer is involved in and where that business operates. The CRA is essential in satisfying this requirement. Guidance on the CRA can be found at section 2.2.9.

Measures to understand the ownership and control structure of the customer should be sufficient to ensure the relevant person can be reasonably satisfied that it understands the risk associated with the different layers of ownership and control. Relevant persons should be satisfied that:

- the ownership and control structure of the customer is not unduly complex or opaque; or
- complex or opaque ownership and control structures have a legitimate legal or economic reason.

Information to understand the ownership and control structure of the customer could include structure charts and lists detailing the persons as described above plus details of the group's structure and any connected entities as appropriate.

Relevant persons must be vigilant as to whether a customer's ownership and control structure could give rise to ML/FT/PF suspicions.

Code 12(7), 12(2) - (6) 13, 21(1)

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 [including foundations] 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.

Code 4(2), 12(7)(b)

Where a payment such as a distribution or loan is made to ~~an~~a third party on behalf of a beneficiary or beneficial owner, that third party must be identified and subject to materiality and risk, their identity verified[10]. The risk based approach allows flexibility, firstly in respect of the extent of identification information obtained and secondly when considering verifying the recipient or beneficiary's identity,

[10] Appropriate procedures and controls must be in place to ensure the recipient or beneficiary is not on a sanctions list as defined in the Code.

provided the procedures undertaken enable the relevant persons to manage and mitigate their ML/FT/PF risks.

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

The relevant person must be satisfied with the CDD obtained on the recipient or beneficiary before making the payment. 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;
- paying an invoice on behalf of a beneficiary or beneficial owner; or
- payments relating to invoices or loans between third parties (third party payments).

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 of insurance policies and pension schemes see the relevant sector guidance.

3.4.6 Ongoing monitoring procedures and controls

Code 4(1), 13

Relevant persons must establish, record, operate and maintain procedures and controls to ensure they comply with the ongoing monitoring requirements at paragraph 13 of the Code. There are several different ongoing monitoring requirements each with their own particular needs and challenges. The procedures and controls necessary to satisfy the requirements for CDD/ECDD, sanctions and transaction monitoring respectively do not necessarily satisfy each other's needs. Ongoing monitoring procedures and controls should therefore be tailored to the particular requirement.

Code 4(2), 5, 6, 7

Ongoing monitoring is integral to a number of Code requirements including CDD/ECDD requirements and disclosure requirements. It is also integral to the CRA, BRA and TRAs' cycles of information gathering, assessment and review to ensure the relevant person's procedures and controls have adequate regard to the ML/FT/PF risks they face and the relevant person continues to be able to manage and mitigate those risks.

Findings from ongoing monitoring should be documented and kept on file such that they feed into the CDD/ECDD already held and the risk assessments.

Guidance on the interplay between ongoing monitoring and risk assessments is at section 2.2.6.

Relevant persons should also consider how to prevent, or if this is not possible, perhaps due to the size of the relevant person, manage and mitigate the potential for conflicts of interest arising. Separating ongoing monitoring functions from client relationship management, sales or transaction processing may assist.

Code 4

In developing procedures and controls for ongoing monitoring, relevant persons must be cognisant that they are ultimately responsible for ensuring compliance with the Code and other AML/CFT/CPF requirements and their procedures and controls must enable them to manage and mitigate their ML/FT/PF risks.

3.4.6.1 Due diligence monitoring procedures

Code 13(1)(a)

13 Ongoing monitoring

(1) A relevant person must perform ongoing and effective monitoring of any business relationship or occasional transaction, including -

(a) a review of information and documents held for the purpose of customer due diligence and enhanced customer due diligence to ensure they are up-to-date, accurate and appropriate, in particular where the transaction or relationship poses a higher risk of ML/FT;

Procedures and controls for reviewing information and documents to ensure they are up-to-date, accurate and appropriate should be designed with a view to ensuring the customer's circumstances continue to be understood by the relevant person after the initial understanding gained at the outset of the relationship/transaction. It does not necessarily mean that relevant persons must automatically replace, for example, identity verification documents simply because they have expired since they were first obtained. Though, depending on the outcomes from the risk assessments, it may be deemed necessary. Guidance on change of CDD information can be found at section 3.3.6.

The Code acknowledges that procedures and controls for ongoing monitoring of CDD/ECDD must be risk sensitive, focusing on where there are higher risks and targeting resources to where there is greatest need.

Procedures and controls to ensure CDD/ECDD is reviewed and remains up-to-date, accurate and appropriate should include the factors listed below.

- Ensuring that customer contact is proactively used as opportunities to update CDD/ECDD or develop understanding of other information such as changes in the customer or the business relationship (for example apparent changes in the source of the customer's funds or the customer's ownership structure). This updated CDD/ECDD/other information should be recorded and retained in such a way that it forms part of the relevant person's overall understanding of the customer and is accessible for AML/CFT/CPF purposes, enabling the relevant person to understand whether the ML/FT/PF risk associated with a business relationship/transaction has changed.

Code 13(4)

- Setting a date for periodic CDD/ECDD reviews on a risk sensitive basis. The depth and breadth of CDD/ECDD to be reviewed and the frequency of such reviews being determined per the risk assessments, where higher risk customers are reviewed more frequently and to a greater degree in more detail.

- Undertaking CDD/ECDD reviews as a consequence of trigger events. In these situations, it may not always be necessary to re-apply all CDD measures, to the customer. Relevant persons should determine which elements of CDD to apply and the extent of the CDD measures to be applied. For example, the relevant person may determine that only the trigger event itself requires a full review, or it may be that information obtained during the course of the business relationship is all that is necessary to update the CDD held on the customer.

  Examples of trigger events and training to enable staff to recognise and interpret other potential trigger events associated with their customers should be provided in the procedures. Examples of trigger events in the procedures should also be reviewed and revised by relevant persons to ensure they remain appropriate according to the relevant person's risk assessments.

Code 14(1)

- Screening undertaken on all customers (both new and established) to identify new or ongoing relationships/transactions with PEPs. Per paragraph 14(1) screening will need to include any customer, any natural person having power to direct the activities of a customer, any beneficial owner or known beneficiary or, in relation to life assurance policies, any beneficial owner of a beneficiary.

  Screening might also include performing searches not necessarily relevant to establishing PEP status, for example whether there is negative information from a credible source concerning the customer's (or any relevant connected person's) reputation. The guidance on risk assessments, in particular that on sources of information at section 2.2.4.1.1 and the CRA risk factors and considerations at section 2.2.9.2 is relevant.

Code 10(3), 14(2) – (5), 15

- Instructions for staff of the actions to be taken where:
  - CDD is found to be out-of-date, inaccurate or inappropriate; or
  - a CDD review indicates and/or requires a customer to be re-classified as higher risk and/or a PEP and/or where previously applied concessions are no longer available.

    Actions could include:
    - obtaining up-to-date, accurate and appropriate CDD;

- obtaining ECDD/fulfilling the PEP requirements;
- ensuring other relevant staff are made aware of the situation/revised customer status, including with regard to connected account/relationships;
- ensuring relevant senior management approvals are put in place; and
- ensuring any previously applied concessions are no longer relied on and the necessary CDD/ECDD obtained.

- Independent reviews of CDD/ECDD.

Guidance on the frequency of ongoing monitoring is provided at section 3.4.6.

3.4.6.2 Sanctions monitoring procedures

Code 4(1)(a)

4 Procedures and controls

(1) A relevant person must not enter into or carry on a business relationship, or carry out an occasional transaction, with or for a customer or another person unless the relevant person -

(a) establishes, records, operates and maintains procedures and controls –

(ii) in relation to determining whether a customer, any beneficial owner, beneficiary, introducer or eligible introducer is included on the sanctions list;

Code 13(1)(c)

13 Ongoing monitoring

(1) A relevant person must perform ongoing and effective monitoring of any business relationship or occasional transaction, including -

(c) monitoring whether the customer, beneficial owner, beneficiary, introducer or eligible introducer is listed on the sanctions list.

Code 3(1)

3 Interpretation

(1) In this Code -

"sanctions list" means the list of persons who are subject to international sanctions which apply in the Island which is maintained by the Customs and Excise Division of the Treasury.[11]

Procedures for ongoing monitoring in the context of sanctions lists should be capable of detecting when a customer—. involved in an existing business relationship or occasional transaction becomes listed on a sanctions list. Periodic or trigger event customer reviews may not be adequate to detect such listings in

[11] Following the UK's exit from the European Union, 'sanctions list' has the following meaning - the list of persons who are subject to international sanctions which apply in the Island, and which are published by HM Treasury.

a timely manner such that the relevant person does not breach sanctions requirements.

Relevant persons should have clear procedures and controls for staff regarding the actions to be taken should a customer be listed on the sanctions list.

Further guidance and information on the international sanctions applying in the Isle of Man is maintained by ~~IOMCE~~IOMCI.

3.4.6.3 Transactions/Activities monitoring procedures

Code 13(1)(b), 5, 6, 7

13 Ongoing monitoring

(1) A relevant person must perform ongoing and effective monitoring of any business relationship or occasional transaction, including -

(b) appropriate scrutiny of transactions and other activities to ensure that they are consistent with –

(i) the relevant person's knowledge of the customer, the customer's business and risk profile and source of funds of the transaction;

(ii) the business risk assessment carried out under paragraph 5;

(iii) the customer risk assessment carried out under paragraph 6;

(iv) any technology risk assessments carried out under paragraph 7; and

Code 13(2), (3)

The purpose of monitoring transactions/activities is ultimately to identify transactions/activities that are or could be ML/FT/PF. To this end, ongoing monitoring procedures and controls must be capable of identifying unusual transactions/activities and suspicious transactions/activities. In order to be able to identify unusual or suspicious transaction/activity, relevant persons must understand what is expected to occur during the business relationship/occasional transaction and conversely, what is inconsistent with that.

The Code's requirement to conduct appropriate scrutiny of transactions/activities to ensure consistency is a twofold requirement referring to both the relevant person's knowledge of that specific customer (including the CRA), as well as the wider context of the relevant person's BRA and TRA. Transaction monitoring can only be effective where a relevant person has a fully developed and integrated understanding of both these areas and how the transactions/activities undertaken in respect of a particular business relationship/occasional transaction compare with these baselines.

Code 8(3), 11(3)

A relevant person's knowledge of the specific customer, will derive from the CDD/ECDD obtained at the outset of the relationship, any information obtained particular to the CRA and any CDD/ECDD or CRA updates. The effectiveness of any subsequent monitoring is directly linked to the adequacy of the information gathered and the relevant person's understanding of that information. Of particular importance when scrutinising transactions/activity to determine

whether the relationship/transaction is as expected is information obtained about the nature and intended purpose of the business relationship/occasional transaction and the source of funds.

Guidance on the nature and intended purpose of a business relationship/occasional transaction is at section 3.7.
Guidance on source of funds is at section 3.8.1.

Performing ongoing monitoring against the backdrop of the relevant person's BRA and TRA provides a broader context enabling the relevant person to compare the transactions/activities of a particular customer against similar customer types, products/services.

Procedures and controls to ensure effective and appropriate transaction monitoring should be relative to the nature, size and complexity of the relevant person's business and their ML/FT/PF risks. When devising their procedures and controls, relevant persons should:

- determine which transactions/activities they will monitor in real time and which transactions they will monitor after the fact. In making these decisions, relevant persons should determine which high-risk factors or combination of high-risk factors will always trigger real-time monitoring and which transactions associated with higher ML/FT/PF risk are monitored in real time, in particular where the risk associated with the business relationship is already increased;
- determine whether they will monitor transactions/activities manually, or using an automated transaction monitoring system. Relevant persons that process a high volume of transactions should consider putting in place an automated transaction monitoring system;
- ensure processes are in place to review flagged transactions/activities without undue delay; and
- perform regular reviews on a random sample taken from all processed transaction/activities to identify trends that could inform their risk assessments and to test the reliability and appropriateness of their transaction monitoring system.

Relevant persons should be vigilant for any changes in the nature of the business relationship with the customer over time. This may include where:

- new products/services are entered into;
- new corporate or trust structures are created;
- a change in a customer's employment or other circumstances takes place;
- the stated activity or turnover of a customer increases; or
- the nature, volume or size of transactions increases etc.

3.4.6.4 Unusual activity and actions that must be taken when unusual activity is identified

Code 3(1)

3 Interpretation

(1) In this Code –

"unusual activity" means any activity including the receipt of information during the course of a business relationship, occasional transaction or attempted transaction where –

(a) the transaction has no apparent economic or lawful purpose, including a transaction which is -

(i) complex;

(ii) both large and unusual; or

(iii) of an unusual pattern;

(b) the relevant person becomes aware of anything that causes the relevant person to doubt the identity of a person it is obliged to identify; or

(c) the relevant person becomes aware of anything that causes the relevant person to doubt the good faith of a customer, beneficial owner, beneficiary, introducer or eligible introducer.

Whether activity is identified as unusual depends on the knowledge a relevant person has developed about their customer from their initial and ongoing CDD/ECDD, CRA and CRA reviews and the context of that customer relative to the BRA. However, situations that are likely to appear unusual include, but are not limited to:

- transactions, activity or instructions which have no apparent legitimate purpose and appear not to have a commercial rationale;
- transactions, activity or instructions that involve apparently unnecessary complexity;
- where the size or pattern of transactions is out of line with expectations for that customer;
- where the customer is not forthcoming with information about their activities, for example, reason for a transaction, source of funds, CDD documentation;
- where the customer who has entered into a business relationship uses the relationship for a single transaction, or only for a very short period of time, where that was not expected;
- the extensive use of offshore structures where the customer's needs are inconsistent with the use of such services;
- transfers to or from high risk jurisdictions which are not consistent with the customer's expected activity;
- unnecessary routing of funds through third party accounts;
- unusual investment transactions with no discernible purpose; and

- extreme urgency in requests from the customer, particularly where they are not concerned by factors such as large transfer fees and early repayment fees.

When unusual activity is identified relevant persons must take action in three ways, as detailed below.

Code 13(2)(a), 3(1), 13(2), 15

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;

The purpose of procedures to scrutinise unusual activity is to gain a better understanding of the customer and their activity and to determine whether or not the activity is suspicious.

Appropriate scrutiny of unusual activity means the relevant persons should take specific, detailed measures to examine the unusual activity that has been identified. In order to be "appropriate", the depth and extent of scrutiny needed will be relative to the nature, volume/size, complexity and scope of the activity and the risk factors concerned. When determining which sources of information to use when conducting scrutiny, relevant persons should be mindful of the principles set out in section 3.3.4 Relevant persons must always ensure that in respect of any particular case, their procedures enable them to manage and mitigate their ML/FT/PF risks. It is for relevant persons to determine their procedures and what measures are appropriate in any particular case, but measures could include (but are not limited to):

- comparing the unusual activity against the customer's CDD (including the nature and purpose of the business relationship/occasional transaction and source of funds) obtained at the outset of the business relationship/occasional transaction and during the course of the business relationship;
- taking reasonable measures to understand the background and purpose of the specific unusual activity, for example by:
  - seeking an explanation of the activity from the customer;
  - seeking supporting documents/data/information whether from the customer themselves/itself and/or from other sources;
  - comparing the customer's explanation with ~~publically~~publicly available information, for example if a large credit supposedly relates to the sale of a house, consider checking the address and average prices in that area;
  - establishing the source of the particular funds used and the destination of the funds;
  - finding out more about the customer's business;

- obtaining an understanding of the relationships between the customer and any related parties;
- examining other connected customers, accounts or relationships for example, linked accounts, introducers/eligible introducers, or connected individuals, such as beneficial owners, beneficiaries, controllers, signatories or other third parties; and
- considering the information obtained or held against known typologies and high-risk indicators – transaction type, customer background, location and currency.

Code 13(2)(b), 3(1), 15

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-

(b) conduct enhanced customer due diligence in accordance with paragraph 15; and

Code 3(1), 13(2), 15

In addition, ECDD must be undertaken. This is not limited to ECDD on the activity alone, but covers the full range of ECDD steps outlined at paragraph 15. Relevant persons should be particularly mindful of anything which causes them to doubt the identity of a person they are obliged to identify or that causes them to doubt the good faith of a customer, beneficial owner, beneficiary, introducer or eligible introducer.

Guidance on ECDD is as section 3.4.7.

Code 13(2)(c) 3(1), 15

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-

(c) consider whether to make an internal disclosure.

Code 3(1)

3 Interpretation

(1) In this Code –

"internal disclosure" means a disclosure made under paragraphs 25(c) (reporting procedures) and 26 (internal disclosures);

Code 13(2)(c), 25(c), 26(b)

Persons scrutinising the unusual activity should consider whether they should make an internal disclosure to the MLRO. Where, at any stage (whether before, during or after scrutiny of the activity and ECDD has been undertaken), the relevant person identifies any suspicious activity or information or other matters that are in their opinion suspicious activity, that person must make an internal disclosure to the relevant person's MLRO.

The need to search for information should not delay making an internal disclosure where suspicious activity is identified.

Matters likely to cause suspicion after conducting appropriate scrutiny include, but are not limited to:

- the customer is unable, or refuses, to provide a reasonable explanation for the activity and this is perceived as being an attempt to conceal criminal conduct rather than the customer being awkward, unhelpful or secretive for personal reasons;
- the explanation does not match the facts or does not make economic sense;
- independent data sources reveal negative information on the customer or related parties such as allegations of corruption; or
- activity appears consistent with known ML/FT/PF typologies.

Guidance on making internal disclosures is at section 5.4.

Code 4(2), 5(2), 6(2), 7(2)

Relevant persons should review the information they hold to ensure that any new or emerging information that could affect their risk assessments is identified and incorporated in a timely fashion in order to ensure the risk assessments remain up-to-date.

Guidance on risk assessments is at section 2.2

3.4.6.5 Ongoing monitoring requirements when activity is identified as suspicious

Code 13(3), 15, 3(1)

13 Ongoing monitoring

(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, unless the relevant person reasonably believes conducting enhanced customer due diligence will tip off the customer; and

(b) make an internal disclosure.

Code 3(1)

3 Interpretation

(1) In this Code –

"suspicious activity" means any activity, including the receipt of information, which in the course of a business relationship, occasional transaction or attempted transaction causes the relevant person to –

(a) know or suspect; or

(b) have reasonable grounds for knowing or suspecting,

that the activity is ML/FT or that the information is related to ML/FT;

Guidance on conducting ECDD is at section 3.4.7.
Guidance on suspicious activity and making internal disclosures is at section 5.4.

3.4.6.6 Extent and frequency of monitoring – ongoing monitoring programmes

Code 13(4), Part 3

13 Ongoing monitoring

(4) The extent and frequency of any monitoring under this paragraph must be determined –

(a) on the basis of materiality and risk of ML/FT;

(b) in accordance with the risk assessments carried out under Part 3; and

(c) having particular regard to whether a customer poses a higher risk of ML/FT.

Code 4 – 7, 13(4), 14, 15

Ongoing monitoring procedures must include the relevant person's documented monitoring programmes. It is for relevant persons to determine the extent (depth and breadth) and frequency of their monitoring broadly and in relation to any particular case according to their risk assessments and the requirements of paragraph 14 and 15 of the Code. This may mean that monitoring programmes vary from case-to-case and/or from one customer type to another. Considerations when developing ongoing monitoring programmes and procedures include:

For CDD/ECDD

Where there are lower risks, the frequency of CDD reviews could potentially be carried out only when there are trigger events such as the customer looking to take out a new product or services or when a certain transaction threshold is reached. Relevant persons must ensure that this does not mean the CDD information is never reviewed or updated.

Where there are standard or higher risks, periodic reviews could be undertaken more frequently according to the assessed ML/FT/PF risks. In addition, the reviews could be more in-depth and detailed, requiring more robust information, documents and/or data.

Code 4 – 8, 13

For SOF

Where periodic reviews and ongoing monitoring are undertaken, consideration should always be given to identifying any missing or inadequate SOF information. This is particularly important when dealing with legacy customers where, due to the age of the relationship, there may be insufficient SOF information on file.

It is acknowledged that difficulties do arise when trying to obtain SOF information for legacy customers and that requesting and obtaining historic SOF information to satisfy current requirements may be a challenge, however, all reasonable efforts should be made to update where missing or inadequate SOF information is identified. The success or limitation of this should be clearly articulated and documented on a customer's file.

Code 4 – 13, 15

For SOW

Where periodic reviews and ongoing monitoring are undertaken in respect of customers who are assessed as higher risk, consideration should always be given to identifying any missing or inadequate SOW information. This is particularly important when dealing with legacy customers where, due to the age of the relationship, there may be insufficient SOW information on file.

SOW information should be as up to date and accurate as possible and should provide a clear understanding of the wealth of a customer and how this wealth was generated.

It is acknowledged that difficulties may arise when trying to obtain SOW for legacy customers, especially in cases where the wealth was generated historically. All reasonable efforts should be made to obtain satisfactory SOW information in cases where this is deemed necessary, and the success or limitation of this should be clearly articulated and documented on a customer's file.

For transaction monitoring:

Where there are lower risks, the frequency and intensity of transaction monitoring could be adjusted by only monitoring transactions above a certain threshold. Where relevant persons choose to do this, they should ensure the threshold is set at a reasonable level and that they have systems in place to identify linked transactions that, together, would go above the threshold.

Where there are higher risks, transaction monitoring could be more frequent with more attention to detail. Individual transactions could be monitored where this is commensurate with the identified ML/FT/PF risk.

Code 4(2) When determining the extent and frequency of ongoing monitoring programmes and reviews, relevant persons must be mindful of the overarching requirements that their procedures and controls must be risk sensitive, with particular regard to higher risk relationships/transactions and they must enable them to manage and mitigate their ML/FT/PF risks.

Whatever the extent and frequency of reviews is determined to be appropriate for the relevant person's monitoring programmes, they should be undertaken in a timely manner with the outcomes feeding into other relevant procedures and controls (risk assessment, CDD/ECDD, simplified measures etc.) expeditiously.

Code 4(1) Planned monitoring programmes must be appropriately recorded so that staff know when and to what depth monitoring checks are to be undertaken for any particular customer. Whether monitoring programmes are recorded centrally or attached to individual client files is for relevant persons to decide depending on

what they consider will most enable staff to operate the procedure for that particular customer as planned~~,~~ and ensure they can demonstrably meet the Code's requirements.

3.4.6.7 Recording monitoring that has been undertaken

Code 13(5), 33, 34, 35

13 Ongoing monitoring

(5) A relevant person must record the date when each review of the business relationship takes place and details of any examination, steps, measures or determination made or taken under this paragraph.

Relevant persons' procedures must ensure that ongoing monitoring that has been undertaken on a business relationship is properly documented. This includes the process and analysis undertaken for each relationship as well as the outcomes. The information should be recorded and retained in such a way that it forms part of the relevant person's overall understanding of the customer and is accessible for AML/CFT/CPF purposes, enabling the relevant person to understand whether the ML/FT/PF risk associated with a business relationship/transaction has changed.

The results of ongoing monitoring undertaken are vital for determining appropriate procedures for the extent and frequency of future monitoring programmes on business relationships. The results of ongoing monitoring undertaken should be documented in such a way as to aid such determinations.

`

The ongoing monitoring records must be available to the MLRO, Head of Compliance/Compliance Officer, other appropriate staff and competent authorities. For the avoidance of doubt, ongoing monitoring records fall within paragraph 33(a) of the Code as documents obtained or produced under Part 4 and therefore must be retained in accordance with paragraph 34(4).

Guidance on record keeping and retention is at section 6.4.

3.4.7 Enhanced customer due diligence ("ECDD")

3.4.7.1 What is ECDD?

Code 3(1), 15, 8 – 14, 16 – 22, 36, 37, 39

3 Interpretation

(1) In this Code -

"enhanced customer due diligence" means the steps specified in paragraph 15 (enhanced customer due diligence) which are additional to the measures detailed in paragraphs 8 to 14, 16 to 22, 36, 37 and 39 for the purpose of identifying and verifying the identity of customers, any beneficial owners and other persons;

Code 9(5)

9 Introduced business

(5) If the risk assessment indicates higher risk, the relevant person must undertake enhanced customer due diligence on the customer in accordance with paragraph

15 including, taking reasonable measures to establish the source of wealth of the customer and any beneficial owner of the customer.

Code 15(1)

15 Enhanced customer due diligence

(1) A relevant person must establish, record, maintain and operate appropriate procedures and controls in relation to undertaking enhanced customer due diligence.

(2) Enhanced customer due diligence includes –

(a) considering whether additional identification information needs to be obtained and, if so, obtaining such additional information);

(b) considering whether additional aspects of the identity of the customer need to be verified by reliable independent source documents, data or information and, if so, taking reasonable measures to obtain such additional verification;

(c) taking reasonable measures to establish the source of wealth of the customer;

(d) undertaking further research, where considered necessary, in order to understand the background of a customer and the customer's business; and

(e) considering what additional on-going monitoring should be carried out and carrying it out.

Code 4(2)

These steps are not exhaustive. Other steps may also be appropriate depending upon the particular circumstances of the business relationship/occasional transaction. Enhanced requirements are relative to what the relevant person already does as standard meaning it is for relevant persons to determine what ECDD is appropriate on a case-by-case basis taking into account the higher ML/FT/PF risk and the overarching requirement that their procedures and controls must enable them to manage and mitigate the higher ML/FT/PF risks.

Enhancements of the standard CDD and ongoing monitoring requirements and the standard procedures and controls established and maintained by each relevant person include obtaining more information/documentation, to a broader degree or a greater depth, more frequently.

In respect of enhanced/additional ongoing monitoring this could include obtaining information on the reasons for intended or performed transactions, increasing the number and timing of controls applied, and selecting patterns of transactions that need further examination.

Guidance on identifying and verifying identity is at sections 3.5 and 3.6, and guidance on ongoing monitoring is at section 3.4.6.
Guidance on source of wealth is at section 3.8.5.

Relevant persons should be aware that the information requirements may be subtly different depending on the particular business relationship/occasional transaction and the potential risks involved. ML involves the proceeds of crimes which have already taken place, but this does not mean that the source of the funds is necessarily "dirty". For example, funds could be coming from a "clean" source, but on their way to a fraudster who is defrauding the person from whom the funds are coming. 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. Relevant persons should also be aware that in FT, monies may be used to buy otherwise innocuous items such as backpacks, rail or bus tickets etc. Not all FT is large value "funding".

In undertaking ECDD 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.

Code 15(1)

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 ECDD requirements in the Code have been met.

3.4.7.2 When ECDD must be carried out and removal of Code concessions

Code 15(3), 9(5)

15 Enhanced customer due diligence

(3) A relevant person must conduct enhanced customer due diligence –

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

Code 6(3)(d), 15(5), (7)

This requirement applies both when a new customer is assessed as higher ML/FT/PF risk by the CRA and when a CRA review is undertaken for an existing customer.

Code 8(2), 11(2)

ECDD for a new customer must be undertaken in line with the timing of ID&V requirements at paragraphs 8(2) and 11(2) of the Code i.e. before a business relationship or occasional transaction is entered into or during the formation of a relationship.

Code 4(2), 15(8)

Where an existing customer is subsequently assessed by a CRA review as posing a higher ML/FT/PF risk, the ML/FT/PF risks are heightened because the relationship is already established and activities have already commenced. ECDD measures must be conducted within a reasonable timeframe. What is considered a "reasonable timeframe" in any particular case is for the relevant person to determine ensuring it is documented and can be demonstrably justified in every case. Relevant persons must also ensure that, where existing customers are assessed as higher ML/FT/PF risk but the ECDD measures are still in the process of being undertaken, those ML/FT/PF risks are managed and mitigated and they have effective procedures and controls to forestall and prevent ML/FT/PF.

Appropriate procedures and controls should include ensuring that the amount, type and number of transactions/activities undertaken for the customer is appropriately limited and monitored. This may mean, depending on the particulars of the case, that it is not appropriate to conduct any transactions or activity until ECDD measures have been completed and the relevant person is satisfied that they can manage and mitigate the higher ML/FT/PF risks identified.

Code 15(5), (7)

Guidance on CRAs and risk assessment reviews is at sections 2.2.9 and 2.2.6. CRAs must have regard to all relevant risk factors including the risk factors included at paragraph 15(5) and paragraph 15(7).

Code 15(3)(b), (c), 13, 26

15 Enhanced customer due diligence

(3) A relevant person must conduct enhanced customer due diligence –

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

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

Unusual activity and suspicious activity are dealt with in sections 3.4.6.4 and 5.3.1 of the Handbook.

Code 15(4), 15(3)(a), 8(4), 11(4) and (5), 16 - 19, 20(2), (3) and (5), 21

15 Enhanced customer due diligence

(4) For the avoidance of doubt, if higher risk of ML/FT within the meaning of sub-paragraph (3)(a) is assessed, then paragraphs 8(4), 11(4), 11(5), 16 to 19, 20(2), (3), (5) and 21 do not apply.

The paragraphs which do not apply where a higher risk of ML/FT/PF is assessed provide concessions from particular Code requirements as follows:

- Paragraph 8(4) provides a concession on the timing for undertaking verification of a customer's identity – see section 3.4.8;
- Paragraphs 11(4) and 11(5) provide concessions in respect of exempted occasional transactions – see section 4.1;
- Paragraph 16 provides a concession for acceptable applicants – see section 4.2;
- Paragraph 17 provides a concession for persons in a regulated sector acting on behalf of a third party – see section 4.3;
- Paragraph 18 provides a concession for generic designated business – see section 4.4;
- Paragraph 19 provides a concession for eligible introducers – see section 4.5;
- Paragraph 20 provides concessions specific to insurance – see the Insurance Act 2008 sector specific guidance; and

- Paragraph 21 provides various miscellaneous concessions – see section 4.7.

Code 4(2), 5 - 7

When determining whether to approve the establishment or continuation of such a business relationship or occasional transaction, relevant persons must ensure that they are able to manage and mitigate the higher ML/FT/PF risks.

Such determinations are not isolated decisions but must be taken with regard to the ECDD measures undertaken and ECDD obtained. Decisions must also be made in the context of the CRA, BRA and TRAs ensuring such determinations are fed back into the CRA and BRA appropriately.

Relevant persons should document their considerations and determinations in order to be able to demonstrate their basis.

3.4.8 Timing of ID&V

3.4.8.1 Timing in relation to new business relationships and occasional transactions

Code 8(2), (4)

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.

Code 11(2)

11 Occasional transactions

(2) The procedures and controls must be undertaken before the occasional transaction is entered into.

For business relationships only, a concession on this strict timing exists, but only for the verification of identity. This is only where there is little risk of ML/FT/PF occurring.

Code 8(4), (3)(b), (c)

8 New business relationships

(4) In exceptional circumstances the verification of the identity of the customer in accordance with sub-paragraphs (3)(b) and (c) may be undertaken after the formation of the business relationship if –

(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.

Code 8(4)(b)

Procedures for the use of this concession must cover the conditions at 8(4) of the Code. This concession is only allowable in exceptional circumstances and where it is essential not to interrupt the normal conduct of business. Use of the concession must be justified and documented. An example of where this concession may be appropriate 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.

Code 8(4)(c)

This concession is not allowed where a customer is identified as posing a higher risk. The route to identifying higher risk customers lies with the CRA and CRA reviews. Guidance on the CRA is at section 2.2.9.

Code 3(1), 4(2), 8(4)(d), 8(4)(g), 13

Relevant persons must always have regard to the materiality and risk of ML/FT/PF and ensure that their procedures enable them to manage and mitigate their ML/FT/PF risks, including those risks that arise through delayed verification of customer identity. This would include being satisfied that the primary motive for the use of this concession is not for the circumvention of CDD procedures. In addition to the specific monitoring requirements at 8(4)(g), the ongoing monitoring procedures at paragraph 13 of the Code must also be adhered to when availing of this concession. In addition, relevant persons should not repay funds to the customer or a third party until the verification procedures have been completed.

Guidance on unusual and suspicious activity is at sections 3.4.6.4 and 5.3.1.

The relevant person should document the use of this concession including its justification for using it.

3.4.9 Timing in relation to continuing business relationships

Code 10(2)

10 Continuing business relationships

(2) The procedures and controls must be undertaken during a business relationship as soon as reasonably practicable.

Code 10

The requirements of paragraph 10 cover the scenario where new Code requirements are introduced for existing sectors already subject to the Code. It also includes any business relationships held prior to AML/CFT/CPF requirements

coming in for a particular business sector. It is anticipated this will only affect a small number of relevant persons.

The Authority issued guidance in October 2019 which specified that information should be obtained within 6 months of the 2019 Code coming into effect (by December 2019). Flexibility was provided for relevant persons to extend this period where they had a particularly large customer base and 6 months was impractical. In such cases, the rationale should have been documented and the Authority informed of the relevant person's proposed timetable to remediate this. The Authority should be informed if this timetable lapses.

Guidance on record keeping is at section 6.4.

3.4.10 Unable to meet CDD/ECDD requirements

The CDD process once begun, must be pursued through to conclusion within a reasonable timeframe. If a prospective customer does not pursue an application, CDD/ECDD requirements cannot be met or verification concluded without adequate explanation, the following requirements apply:

Code 8(5), 9(9), 10(5), 11(7), 12(11), 14(6), 15(8), 19(11)

8 New business relationship, 9 Introduced business, 10 Continuing business relationships, 11 Occasional transactions, 12 Beneficial ownership and control, 14 Politically exposed persons, 15 Enhanced customer due diligence, 19 Eligible introducers

- the business relationship or occasional transaction must proceed no further / the occasional transaction is not to be carried out;
- the relevant person must terminate the business relationship / the relevant person must consider terminating that/the business relationship; and
- the relevant person must consider making an internal disclosure.

Relevant persons must refer to the relevant Code paragraph for the specific requirements applicable.

Code 34(4)

In these circumstances, all information and documentation that has been obtained must be retained for at least 5 years from the relevant date.

Code 4(2), 9(9), 10(5), 12(11), 14(6), 15(8), 19(11)

In allowing relevant persons to consider terminating a business relationship which has already commenced, the Code acknowledges that there are particular business relationships which it may not be possible legally to terminate once commenced. In considering whether to terminate, relevant persons must take a risk based approach, ensuring that they can manage and mitigate their ML/FT/PF risks.

Guidance on making internal disclosures is at section 5.4.

3.5 Identifying the customer, beneficial owner and other related parties

Code 8(3)(a), 11(3)(a), 12
POCA s180, 181
ATCA Sch 6
POC (Pres Disc) Order 2015 Schedule

Relevant persons must identify the customer (and other persons per paragraph 12 of the Code). Identification requires relevant persons obtain identity information to enable the relevant person to know who their customer is. At this stage, no identity verification (whether that be in the form of documents, data or information) is collected. The Code does not, for the most part, prescribe what pieces of identity information relevant persons must obtain. Relevant persons must note, that POCA and ATCA define "customer information" in the context of customer information orders which may be used in ML/terrorist investigations. In addition, the Proceeds of Crime (Prescribed Disclosures) Order 2015 ("POC (Pres Disc) Order 2015") contains information that must be submitted when making a disclosure. The guidance provided on customer identity takes account of these requirements, thought relevant persons must also refer to the relevant legislation.

Code 4(2), 15(2)(a)

The risk based approach allows flexibility in respect of the extent of identity information to obtain on a case-by-case basis, subject to other legal (including AML/CFT/CPF) obligations, a relevant persons' risk assessments and provided ML/FT/PF risks are effectively managed and mitigated. Consequently, where there are higher ML/FT/PF risks, relevant persons must consider whether additional identity information is needed and obtain it.

It is for relevant persons to make their own reasoned judgements in any particular case as to the extent of identity information to gather, and it is for relevant persons to ensure they can justify their decisions. Adequately recording the decisions taken as well as the reasons for the decisions is essential in enabling relevant persons to do this.

POCA s180, 181, ATCA Sch 6 para 7
POC (Pres Disc) Order 2015 Schedule

To assist relevant persons' understanding of what information comprises identity, non-exhaustive lists are included for various customer types. Such information can be obtained from the customer themselves or from any other source. Items marked with an "*" are listed within: POCA and ATCA's definitions of "customer information", the POC (Pres Disc) Order 2015 as information that must be submitted when making a disclosure; or as specific Code requirements. These items are the minimum identity information that relevant persons must collect.

Relevant persons should also note the customer information that must be submitted in a disclosure if it is known or held by the relevant person per the POC (Pres Disc) Order 2015.[12]

3.5.1 Natural persons

Identity is the specification of a unique natural person that is based on characteristics of the person that establish a person's uniqueness in the population or particular context; and is recognised by the state for official purposes.

[12] It must be ensured this is obtained in relation to new customers, and where it has not been obtained for existing customers ~~should be obtained~~, consider obtaining this as part of ongoing monitoring processes.

Code 12(2) POCA s181(2) ATCA Sch 6 para 7 POC (Pres Disc) Order 2015 Schedule

- *title
- *full name (forename(s) or initials and surname);
- any former names (e.g. maiden name);
- any other names used;
- *date of birth;
- *place of birth;
- *most recent address and *any previous addresses. This refers to the person's permanent residential address (including post code if possible). A PO Box address does not constitute identity information. In addition, where "care of" addresses are used, relevant persons should consider the risks and how to mitigate them as part of their CRA;
- other contact details such as telephone number and email address;
- nationality (including any other nationalities);
- *gender (being either male, female or unknown);
- an official personal identification number or other unique identifiers contained in an un-expired official document.
- occupation and name and address of employer/source of income;
- details of any public or high profile positions held; and
- *identification information on other persons per paragraph 12 of the Code (see guidance on Beneficial Ownership and Control at section 3.4.5).

3.5.2 Legal arrangements

Code 12(3), (6) POCA s181 ATCA Sch 6 para 7 POC (Pres Disc) Order 2015 Schedule

- *identity information for the trustees. The legal status of the trustee (i.e. whether natural or legal person) will determine what is identity information;
- *name and address of any other natural persons controlling or having power to control the customer (as above);
- *name of arrangement;
- date of establishment;
- situs of arrangement i.e. the state whose courts have primary jurisdiction over the trust;
- legal status of the arrangement (where applicable);
- official identification number where applicable (e.g. tax identification number or registered charity number); and
- *identification information for any other persons per paragraph 12 of the Code (see guidance on Beneficial Ownership and Control at section 3.4.5).

3.5.3 Foundations

POCA 181(3) ATCA Sch 6 para 7 Code 12

- *full name of foundation;
- *country or territory in which it is incorporated/established/registered;

- *any number allocated to it under the statutory provision under which it is incorporated/established/registered or corresponding legislation of any country or territory outside the Island;
- date of incorporation/registration/establishment;
- *any number assigned to it for the purposes of value added tax in the Island or the UK;
- *registered office/business address and any *previous registered offices/business addresses;
- principal place of business/operations (if different from registered office);
- mailing address (if different from registered office);
- other contact details such as telephone number and email address;
- *the statutory provision under which it is incorporated or established or anything similar under corresponding legislation of any country or territory outside the Island;
- *full name, date of birth and most recent address and any previous addresses of any person who is a signatory to the account or any of the accounts;
- *identification on other persons per paragraph 12 of the Code (see guidance on Beneficial Ownership and Control); and
- *a description of any business which the person carries on.

3.5.4 Legal persons

POCA s181(3)
ATCA Sch 6 para 7
Code 12

- *full name of entity;
- any trading names;
- type of legal person;
- *country or territory in which it is incorporated/established/registered;
- *any number allocated to it under the statutory provision under which it is incorporated/established/registered or corresponding legislation of any country or territory outside the Island;
- date of incorporation/registration/establishment;
- *any number assigned to it for the purposes of value added tax in the Island or the UK;
- *registered office address and any *previous registered offices;
- principal place of business/operations (if different from registered office);
- mailing address (if different from registered office);
- other contact details such as telephone number and email address;
- *the statutory provision under which it is incorporated or established or anything similar under corresponding legislation of any country or territory outside the Island;
- whether listed and if so, where;
- name of regulator (if applicable);

- *full name, date of birth and most recent address and any previous addresses of any person who is a signatory to the account or any of the accounts;
- *identification information on other persons per paragraph 12 of the Code (see guidance on Beneficial Ownership and Control at section 3.4.5); and
- *a description of any business which the person carries on.

3.6 Verifying identity

Code 8(3)(b), 9(7), 10(3), 11(3)(b), 12

Relevant persons must verify the identity of their customers and take reasonable measures to verify the identity of beneficial owners (and other persons per paragraph 12 of the Code). Verification of identity, requires relevant persons to check independent, reliable source documents, data or information that confirms the veracity (or otherwise) of the identity information obtained during the identification process.

Whenever verification is obtained, evidence should be retained to show that it has been satisfactorily undertaken. Relevant persons should ensure they are satisfied with the authenticity of any documents, data or information used in the verification process.

Code 4(2), 5 - 7

For the most part, the Code does not prescribe which pieces of identity information must be verified and nor does this guidance, except where explicitly required by the Code or other legal (including AML/CFT/CPF) obligations. Relevant persons should note that the identity items marked with an "*" in section 3.5, should be verified. The risk based approach allows flexibility regarding the extent of verification measures to undertake, such as which specific pieces of identity information to verify and methods to use.

Code 15(2)(b)

It is for relevant persons to determine the extent of verification measures in any particular case relative to the materiality and risk of ML/FT/PF. The risk assessments are vital in these decisions. Consequently, where there are higher ML/FT/PF risks, relevant persons must consider whether additional aspects of identity need to be verified and/or more extensive measures taken, and if so obtain this additional verification. Relevant persons must ensure they can justify their decisions. Adequately recording the decisions taken as well as the reasons for the decisions is essential in enabling relevant persons to do this.

Different types of customer or person(s) connected to the customer (such as natural persons, legal arrangements, and legal persons (including foundations)) will have different verification needs and possible solutions. In some cases, a relevant person may be satisfied the customer is who they say they are without needing to verify all components of identity. Whatever steps are taken to verify identity, relevant persons must ensure, they are satisfied the customer is who they say they are. The steps taken must enable the relevant person to manage and mitigate their ML/FT/PF risks.

The Supplemental Information Document provides further information about verification of identity for relevant persons needing further assistance.

3.6.1 Specific aspects of identity prescribed in the Code requiring verification

Code 8(3)(c), 11(3)(c)

> **8 New business relationships, 11 Occasional transactions**
> (3) Those procedures and controls are –
>
> (c) verifying the legal status of the customer using reliable, independent source documents, data or information;

This requirement applies to all types of customer. In relation to a legal person, for example, this would require verification of the type of legal person and its current status, i.e. live or otherwise. In relation to the legal status of an arrangement, this would involve verifying the satisfactory appointment of the trustee(s) and the nature of their duties.

Code 12(6)(a)

> **12 Beneficial ownership and control**
> (6) Without limiting sub-paragraphs (2) to (5), in the case of a customer that is a legal arrangement or a legal person the relevant person must –
>
> (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;

Code 4(1), 6, 12(6)

Guidance regarding persons with the power to direct the customer's activities under 12(6)(a) can be found at section 3.4.5.4. In all cases, relevant persons must obtain the names and addresses of all such natural persons. This information is important when conducting the CRA in order to determine whether there could be any higher risk persons, PEPs or persons included on the sanctions list associated with the customer.

Code 4(2), 5, 6

Taking "reasonable measures" to verify these specific aspects of identity (name and address) provides flexibility and what is reasonable is relative to the particular circumstances (see 3.2 and 3.3.3).

Code 4(2), 5 - 7

This requirement does not necessarily mean obtaining and verifying full identification information on each of these natural persons. Whether other specific pieces of identity information should be obtained and verified, is a matter for relevant persons to determine on a case-by-case basis relative to the materiality and risk of ML/FT/PF. The results of the BRA, CRA and TRAs are vital in such determinations. Specific considerations, particularly where there are multiple signatories and/or directors for instance with a large multinational company, or a large international charity, are outlined below (3.6.2).

For those firms that may require further assistance on methods for verifying the natural persons with the power to direct a customer, and/or methods for verifying

identity and address the Supplemental Information Document includes non-exhaustive, non-limited lists of examples.

3.6.2 ID&V where there are multiple signatories/directors

Code 4(2), 5, 6

Considerations when determining the extent of identifying and verifying identity (beyond name and address) where there are multiple directors/signatories could include:

- are there signatories with whom the relevant person frequently interacts or takes instructions from;
- are certain signatories likely to be used to sign off certain activity or transactions and;
- the level of signing powers and whether a signatory's power is deemed to be significant.

This information would usually be determined in a discussion with the customer.

3.6.3 Methods to verify identity and address

Code 4(1), (2)

In order to enable the Code's risk based approach, this guidance does not prescribe methods to verify identity, address or other aspects of CDD. Relevant persons should, within their procedures, establish their own lists of the source documents, data and information they will accept in each case bearing in mind the principles and considerations set out in this document, the relevant person's risk assessments and risk assessment reviews and other obligations such as data protection.

Code 4(1), 30(1)

As with all procedures, such lists must be maintained and monitored to ensure they continue to be appropriate per the risk assessments and any risk assessment reviews, and that the source documents, data and information the relevant person intends to rely on still fulfil their needs. Relevant persons must ensure they are satisfied on an ongoing basis that the documents, data and information listed in their procedures continue to enable them to manage and mitigate their ML/FT/PF risks.

Relevant persons' procedures should detail how frequently and in what circumstances the lists or particular methods on the lists will be reviewed to ensure they still meet their needs. Guidance on monitoring and testing compliance with the Code's requirements is at section 6.1.

The Supplemental Information Document includes non-exhaustive, non-limited lists of examples and, in the case of electronic methods relevant considerations, for relevant persons that may require further assistance on this.

Note that simply using the methods listed does not necessarily mean that the relevant person has complied with their obligations under the Code.

3.7 Nature and intended purpose of business relationship/occasional transaction

Code 8(1), (3) 11(1), (3)

8 New business relationships, 11 Occasional transactions

(1) A relevant person must, in relation to each new business relationship / occasional transaction, establish, record, maintain and operate the procedures and controls specified in sub-paragraph (3).

(3) Those procedures and controls are –

(d) obtaining information on the nature and intended purpose of the business relationship / occasional transaction;

The purpose of obtaining information on the nature and intended purpose of the business relationship/occasional transaction at the outset is to ensure the relevant person understands the economic or other commercial rationale for the business relationship/occasional transaction and the scale of expected activity. This enables the relevant person to understand what should be considered normal activity during the relationship and consequently enable them to monitor the customer's activity and transactions to establish whether the business relationship is operating as expected.

Code 3(1), 13

It is only by understanding what the expected norms of the relationship are, that relevant persons are able to monitor and identify potentially unusual and suspicious activity/transactions.

Code 4(2)

Relevant persons should determine the most appropriate information necessary to enable them to comply with their obligations under the Code, including the overarching obligation that their procedures and controls must enable them to manage and mitigate their ML/FT/PF risks. Unless it is obvious from the product being provided, depending on the customer type, information that could be obtained to assist in meeting the Code requirements include, for example:

- information concerning the customer's/beneficial owner's business activities/occupation/employment (having regard for sensitive activities and trading activities);
- geographical sphere of the customer's/beneficial owner's residence, activities and assets;
- information on the types of financial products/services the customer is looking for;
- expected type, volume, frequency and value of activity;
- expected geographical sphere of the activity;
- details of any existing relationships with the relevant person;

Code 12

- understanding the ownership and control structure of the customer where a legal person, arrangement or foundation, including group ownership where applicable as per paragraph 12 of the Code;
- establishing any relationships between signatories and customers;
- relevant information regarding related third parties and their relationships with/to beneficiaries or e.g. an account; and

- name of regulator (if any).

Code 13(1)(b) This relationship information should be used by the relevant person in any monitoring procedures scrutinising transactions and other activities to ensure consistency between expected activity/transactions and actual activity/transactions. It will therefore need to be sufficiently detailed to enable effective monitoring.

Code 6 As with all CDD obtained in respect of a customer/beneficial owner, the information obtained in respect of the nature and intended purpose of the business relationship/occasional transaction should be incorporated into the CRA. As a business relationship matures and the relevant person learns more about the customer/beneficial owner and their use of the products and services acquired, the relevant person's understanding of the customer should become more rounded. This in turn should be incorporated into CRAs as they are reviewed.

3.8 Source of funds and source of wealth

Source of funds and source of wealth (where appropriate) are key elements in recognising and understanding the ML/FT/PF risks posed by a business relationship / occasional transaction and in managing and mitigating those risks. Recording source of funds (and source of wealth where appropriate) information enables relevant persons to:

- understand the customer's background and financial history;
- understand how and where the capital was generated;
- identify if a customer's transactional activity is in line with what would reasonably be expected based on the information recorded about the customer; and
- assess if the activity and transactions are potentially suspicious.

Code 8, 11, 14, 15 The Code requires relevant persons to take reasonable measures to establish the source of funds for all customers and source of wealth for certain PEPs, where there are higher ML/FT/PF risks, in the event of unusual activity and in the event of suspicious activity, unless the relevant person believes this will tip off the customer.

The requirement is to take "reasonable measures to establish" source of funds and, where necessary, source of wealth, rather than requiring relevant persons to "verify" such. These two terms are distinct. Whereas "verify" requires the use of reliable, independent source documents, data or information in every case, "reasonable measures to establish" allows greater flexibility according to the relative ML/FT/PF risk of the business relationship / occasional transaction. Those "reasonable measures to establish" may therefore range from obtaining information to verifying that information using reliable, independent source documents, data or information, and all the steps in between to enable a relevant person to manage and mitigate their identified ML/FT/PF risks.

"Funds" and "wealth" are two different concepts in the Code, and are discussed as sections 3.8.1 and 3.8.5.

3.8.1 Source of funds

Code 3(1)

3 – Interpretation
(1) In this Code -
"source of funds" means the origin of the particular funds or other assets involved in a business relationship or occasional transaction and includes the activity that generated the funds used in the business relationship or occasional transaction, and the means through which the funds were transferred.

Source of funds, i.e. the amounts being invested, deposited or wired as part of the business relationship / occasional transaction, both at the outset of the relationship and during its course, is a twofold concept:

- the activity(ies) that generated the funds to be used or which concern the business relationship / occasional transaction means the customer's salary, returns on investments, inheritance, sale of assets, income from trading etc.; and
- the means through which the customer's funds are transferred refers to, for example, the funds coming from a bank account in the name of X.

Some categories of relevant person may not receive the funds that concern the business relationship / occasional transaction, due to the nature of the services provided.

POCA Sch 4 2(6)(h)

An example of such a business includes where a legal professional undertakes an activity listed at paragraph 2(6)(h) of Schedule 4 of POCA. The legal professional does not have to receive the funds themselves, nor do the funds have to pass through their client account, for the requirement to take reasonable measures to establish the source of funds concerned in the transaction to apply.

POCA Sch 4 2(6)(o)

A further example can be found with estate agents undertaking activity listed as paragraph 2(6)(o) of POCA. The funds for conveyancing transactions go from one advocate's client account to another advocate's client account and do not pass through the estate agent, but the estate agent is still required to take reasonable measures to establish source of funds of the customer.

3.8.2 Taking reasonable measures to establish source of funds

Code 8(1), (3) 11(1), (3), 15

8 New business relationships, 11 Occasional transactions (1) A relevant person must, in relation to each new business relationship / occasional transaction, establish, record, maintain and operate the procedures and controls specified in sub-paragraph (3).
(3) Those procedures and controls are –

(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(s) 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.

Code 4(2), 3(1)

"Taking reasonable measures to establish source of funds" is a risk based requirement. It means knowing and understanding the ***activities which generated*** these specific funds, ***who provided or will provide the funds*** in the business relationship / occasional transaction and the means through which the funds were ***transferred***.

The depth of research and evidence required to establish source of funds is subject to the materiality and risk of ML/FT/PF. Therefore, the level of work undertaken should vary according to the circumstances of each business relationship / occasional transaction, and be sufficient to enable the relevant person to manage and mitigate identified ML/FT/PF risks.

For example, at the lower risk end of the spectrum it may be reasonable to ask the customer themselves for information about their source of funds without seeking further corroboration or evidence. Conversely, for higher risk customers it may be necessary to further corroborate or verify the information provided in relation to source of funds using reliable, independent source documents. As there are varying degrees of risk associated with business relationships / occasional transactions, there will be varying degrees of what is reasonable between these two extremes. Ultimately, it is a matter for each relevant person to decide what are "reasonable measures" for each business relationship / occasional transaction (or where relevant, category of business relationship / occasional transaction) and be able to justify their decisions and the measures taken.

Code 8(1), (3), 11(1), (3), 33, 34

The flexibility in taking "reasonable measures to establish" source of funds, applies to both the activity(ies) generating the funds to be used in the business relationship / occasional transaction and in respect of the means of transferring the funds (which must be sufficient to ensure reconstruction of the transaction in accordance with paragraph 33(c) of the Code, guidance on this can be found at section 6.4.2). The particular circumstances of the case will dictate whether it is necessary to apply the same level of measures to the activity(ies) as to the means of transfer, or whether a different level is reasonable. Appropriate information and evidence should be obtained and retained on file.

Code 8(5), 9(9), 10(5), 11(7), 12(11), 14(6), 15(8), 19(11)

Where a relevant person is not satisfied that it has established the source of funds, the requirements for non-completion of CDD apply. See section 3.4.10 for further information.

3.8.3 Requirements where funds are received from a third party's account

Code 8(3)(e), 11(3)(e)

Where funds are received from an account not in the name of the customer (third party funding), specific measures must be undertaken for the requirement to take reasonable measures to establish source of funds, to be satisfied.

Code 4(2), 8(3)(e), 11(3)(e), 12

Relevant persons must take a risk based approach to understand the reasons for the third party funding. Where appropriate, relevant persons should make further enquiries about the relationship between the third--party account holder(s) (i.e. the providers of the funds) and the customer and consider beneficial ownership requirements. Consideration must be given to identifying the third--party account holder(s) and taking reasonable measures to verify their identity. In the context of paragraph 8(3)(e)(ii) and 11(3)(e)(ii) of the Code, "identifying the account holder" does not necessarily mean seeking specific identity information such as name, date and place of birth, address etc. for each third party. Depending on the transactions concerned, it may be sufficient to ensure a general understanding that the transactions are in line with expected activity.

Where it appears that the customer is acting on behalf of someone else there is further guidance relating to how to determine this in section 3.4.5.

3.8.4 Ongoing monitoring and source of funds

Code 13

However a business relationship is treated, relevant persons must ensure they comply with the Code's ongoing monitoring provisions, including consideration of source of funds.

Though it may well be necessary, in some cases, for a relevant person to have detailed, evidenced in-depth knowledge of each and every transaction involved in a business relationship, it may not be necessary in all cases. What is reasonable will be a matter for relevant persons to decide in each case. Depending on the relevant person's BRA and CRAs, and their ability to manage and mitigate ML/FT/PF risk, there may be cases where only certain discrete transactions within the business relationship need to be examined in depth (the depth of such examination also being relative to the materiality and risk of ML/FT/PF). There may also be cases where only a broader understanding of the customer's source of funds is necessary.

Such determinations at the outset of a business relationship may be subject to change as the business relationship continues and relevant persons must always be mindful of changing circumstances which may become apparent through, for example, ongoing monitoring and/or BRA and CRA reviews.

3.8.5 Source of wealth

Code 9(5), 14(3), 15(2)(c)

Taking reasonable measures to establish source of wealth is a specified ECDD measure for higher risk customers (including higher risk domestic PEPs) and foreign PEPs.

Code 3(1)

3 Interpretation
(1) In this Code -
"source of wealth" means the origin of a customer's entire body of wealth and includes the total assets of the customer;

Source of wealth is distinct from source of funds and includes the customer's funds that may never have anything to do with the relevant person. It refers to a description of the economic, business/commercial activities that generated or significantly contributed to the customer's overall net worth. It also recognises that the composition of wealth generating activities may change over time as new activities are identified and additional wealth accumulated.

When establishing a customer's source of wealth, it is important firms understand the various figures, values, amounts and time periods associated with and involved in the different generating activities of wealth of the customer.

The following lists non-exhaustive examples of sources of wealth:

Family/generational wealth and personal backgrounds

Includes~~-~~;

- family wealth,
- inheritance,
- gifts (from family, including spouse/partner),
- divorce settlement,
- lawsuit settlement,
- pension or retirement benefit scheme pay-outs,
- casino/lottery wins,
- sales of residential property,
- antiques,
- artwork and
- other personal assets.

Where appropriate, information should be collected on the underlying activities that have generated the wealth.

Income, revenue and business activities

Includes~~-~~;

- business ownership,
- business operations,
- employment,
- sales of products,

- business properties and
- other commercial assets.

For natural persons, examples include salaries, bonuses, commissions and other compensation from employment or contract work, as well as regular income from pension or retirement schemes.

For entities, examples include profits generated from their activities (sales of goods/services), receivables, contracts, existing fixed assets and any periodic funding from existing or new beneficial owners.

Investment activities

Includes~~:~~;

- income from acquisition and sale of investments, e.g. from real estate,
- securities,
- royalties,
- patents,
- inventions and
- franchises.

3.8.6 Taking reasonable measures to establish source of wealth

Code 14(3)

14 Politically Exposed Persons

(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.

Code 15(2), (3)

15 Enhanced customer due diligence

(2) Enhanced customer due diligence includes –

(c) taking reasonable measures to establish the source of the wealth of a customer;

(3) A relevant person must conduct enhanced customer due diligence –

(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.

Reasonable measures to establish source of wealth is about building a broad understanding of a customer's overall sources of wealth. Information can come from the customer and/or other sources and should give an indication as to the volume of wealth the customer has or controls and how such wealth was acquired

(i.e. those activities which have generated a customer's funds and property). It is recognised that it may not always be possible for a relevant person to obtain a complete overview of a customer's entire body of assets, for example in cases where the wealth has been generated across a wide range of activities and over a longer time period. Further, sometimes such information is not voluntarily disclosed. While some gaps in chronology of wealth accumulation over time are not uncommon, any significant gaps and/ or material inconsistencies may present challenges to determining plausibility. A failure to voluntarily disclose such information, when requested, could also be considered a red flag for ML/FT/PF. Relevant persons may be able to gather general wealth information about a customer from commercial databases or other open sources.

Code 4(2)

Source of wealth requirements are risk based and the procedures and practices put in place to satisfy the requirements must enable relevant persons to manage and mitigate their identified ML/FT/PF risks.

Therefore "reasonable measures" in establishing source of wealth for each relevant customer may vary according to the circumstances, with the level of detail obtained and the lengths needed to go to corroborate such information commensurate with the ML/FT/PF risks.

Unlike the source of funds requirements, which are applicable to all customer relationships, source of wealth requirements start from a higher risk threshold because they are particular to customers assessed as posing a higher risk of ML/FT/PF only (though relevant persons may of course seek to establish source of wealth for other customers should they determine it appropriate). This higher risk starting point must be taken into account when considering what source of wealth information, and methods used to establish source of wealth, would be reasonable. However, even with a higher risk starting point, the measures relevant persons take to establish source of wealth should reflect the degree of risk associated with the business relationship, and also what factor(s) are driving that risk level. For example, at the highest level of risk, taking reasonable measures to establish source of wealth means that a relevant person should consider verifying the source of wealth on the basis of reliable and independent data, documents or information.

Code 8(5), 9(9), 10(5), 11(7), 12(11), 14(6), 15(8), 19(11)

Where corroboration proves to be difficult or impossible for the customer, for example, in cases of generational wealth or substantial inheritance received decades ago, the relevant person should assess the plausibility of the information provided and attempt to corroborate key milestones in the customer's wealth history. Factors to consider may include:

- the outcomes of the CRA;
- the quality and plausibility of the information provided as part of the CDD process, the evidence available to corroborate it and whether this reduces (and by how much) the inherent ML/FT/PF risk (e.g.

available evidence indicates the customer's wealth is sufficiently transparent);
- other information held by the relevant person on the customer, including from other lines of business or jurisdictions of operation; and
- market/segment specific governance committees, using experts who understand those markets/segments and any specific considerations that may apply.

Where a relevant person is not satisfied that taking such steps enables them to establish the source of wealth, the requirements for non-completion of CDD apply. See section 3.4.10 for further information.

3.8.7 Researching and verifying source of funds and/or wealth

When researching source of funds and source of wealth, relevant persons should focus on what can be reasonably explained, rather than on what might be expected.

Sources of information which are useful for verifying the accuracy of a customer's declaration about source of funds and/or wealth include, but are not limited to:

- an original or certified copy of a recent pay slip;
- written confirmation of annual salary signed by an employer;
- an original or certified copy of contract of sale of, for example, investments or a company;
- written confirmation of a property sale signed by an advocate or solicitor;
- an original or certified copy of a will or grant of probate;
- written confirmation of inheritance signed by an advocate, solicitor, trustee or executor;
- an internet search of a company registry to confirm the sale of a company;
- publicly available property registers, land registers, asset disclosure registers (particularly in the case of PEPs);
- VAT and income tax returns;
- copies of audited accounts;
- public deeds; and
- independent media reports.

Discrepancies between customer declarations and information from other sources could be indicators of ML/FT/PF activity and should never be disregarded.

3.8.8 Politically Exposed Persons ("PEPs") risk

Much international attention has been paid in recent years to PEPs, with the FATF producing its Guidance – PEPs, 2013. 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 the purpose of committing ML offences and related predicate offences including bribery and corruption as well as conducting activity related to FT. 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.

"Corruption is a complex social, political and economic phenomenon that affects all countries. Corruption undermines democratic institutions, slows economic development and contributes the governmental instability. Corruption attacks the foundation of democratic institutions by distorting electoral processes, perverting the rule of law and creating bureaucratic quagmires whose only reason for existing is the soliciting of bribes. Economic development is stunted because foreign direct investment is discouraged and small businesses within the country often find it impossible to overcome the 'start-up' costs required because of corruption." (UNODC, 2020).

Furthermore, investigations regarding proceeds of corruption often gain publicity and can damage the reputation of both businesses and countries. It is therefore important that relevant persons take their responsibility to identify PEPs seriously.

Being a PEP does not mean that the individual should automatically be stigmatised as involved in criminal activity. A large percentage of PEPs do not abuse their power nor are they in a position to do so. 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/CPF standards, or where they do not meet financial transparency standards. Relevant persons should take appropriate measures to mitigate those risks.

3.8.9 PEP definitions

Code 14(7)

14 Politically exposed persons

(7) In this paragraph –

"domestic PEP" means 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 the location of that PEP, those family members or close associates.

"foreign PEP" means a PEP who is or has been entrusted with prominent public functions outside of the Island and any family members or close associates of the PEP, regardless of the location of that PEP, those family members or close associates.

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. However, should a domestic PEP also fall within the definition of a foreign PEP by virtue of a prominent public function in another jurisdiction, the foreign PEP requirements are applicable.

Code 3(1)

3 Interpretation

(1) In this Code -

"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.

(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 natural person known to be a close associate of P, including –

- (i) a joint beneficial owner of a legal person or legal arrangement, or any other close business relationship, with P;
- (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 a person in a position to conduct substantial financial transactions on behalf of P.

Code 6(2) This definition would include royal families as persons entrusted with prominent public functions. Though the position of honorary consul was removed from the Code's PEP definition relevant persons should remain aware of the potential risks associated with honorary consuls. Relevant persons may choose to identify honorary consuls as PEPs although they are under no obligation to do so.

An "international entity or organisation", referred to at (a)(xi), relates 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 and any affiliated international organisations;
- institutions of the EU;
- the Council of Europe;
- the North Atlantic Treaty Organisation;
- the World Trade Organisation;
- the International Monetary Fund;
- the World Bank; and
- the Organisation for Security and Cooperation in Europe.

3.8.10 PEP requirements

Code 14, 6, 8, 9, 10, 11, 12, 13, 15 For the avoidance of doubt, Code paragraph 14 PEP requirements are additional to other Code requirements such as CRAs, CDD and beneficial ownership, ongoing monitoring and ECDD requirements, which must always be completed irrespective of whether the customer (or related person) is a PEP. The standard CRA and CDD measures are the indispensable starting point which must be applied to any type of customer.

Code 14 While paragraph 14(1) applies to all customers, the controls and procedures required by paragraphs 14(2) - (4) of the Code apply to all foreign PEPs and higher risk domestic PEPs.

Where a relevant person cannot meet the requirements within a reasonable timeframe the requirements for non-completion of CDD apply. Further guidance on this is at section 3.4.10.

3.8.10.1 Determining PEP status

Code 14(1)

14 Politically exposed persons

(1) 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.

Determining whether a customer is a PEP requires relevant persons to take proactive steps. In addition to reviewing CDD information, documents and data a relevant person can utilise various methods, including making enquiries with the customer and consulting commercially available databases and screening tools. Some jurisdictions provide lists of the positions they deem to be prominent public functions within their domestic sphere (the Isle of Man does not have such a list). 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, List C~~In addition, List C and ~~Lists A and B~~Lists A and 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/CPF controls. Consideration should be given to assessing the extent to which an individual could be used by a PEP and the associated risks.

Code 14(1), 13

The obligation to determine whether a customer is a PEP does not end once the customer relationship has been formed. Relevant persons are required to perform ongoing and effective monitoring of any business relationship. Relevant persons should ensure that the procedures for determining whether a customer is a PEP and their ongoing monitoring procedures are clear regarding determining whether any individuals have *become* PEPs since the business relationship was formed.

There is a common misconception that PEPs who have immunity from prosecution and conviction (e.g. Heads of State who, during their term of office, are immune from prosecution for actions committed prior to taking office; or diplomats, who are immune from prosecution and conviction in the countries where they are posted) are exempt from the PEP requirements. This is not the case. Even if a PEP is immune from prosecution and conviction, this does not apply to relevant persons who fail to treat them as PEPs. Similarly, relevant persons are not immune from the requirements to make internal/external disclosures where their suspicions involve a PEP.

Immunity may slow down or prevent the criminal prosecution and conviction of such PEPs, but a disclosure may trigger an investigation which could identify other persons without immunity involved in criminal activity and who could be prosecuted immediately. In addition, the PEP may lose immunity from domestic prosecution at a later stage, at which point a criminal investigation could be opened or continued.

3.8.10.2 Senior management approval

Code 14(2)

14 Politically exposed persons

(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.

Code 8(4)

This requirement applies irrespective of any other CDD timing concessions, such as Code paragraph 8(4).

3.8.10.3 Source of wealth

Code 14(3)

14 Politically exposed persons

(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.

Where a firm identifies that a higher risk domestic PEP, or any foreign PEP, is linked to a customer, but that PEP does not fall within the definition of beneficial owner or fund the business relationship or customer (for instance acting as a Non-Executive Director on a Board) full SOW details may not need to be established. In such circumstances, the relevant person should undertake and document a risk assessment to consider the nature of the PEP's role in order to justify why SOW may not be established in certain circumstances.

Full guidance on the additional requirements to take reasonable measures to establish source of wealth can be found at section 3.8.5.

3.8.10.4 Enhanced monitoring

Code 14(4)

> **14 Politically exposed persons**
> (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.

Code 4(2), 13

This requirement is simply an enhancement of the standard ongoing monitoring requirements at paragraph 13 of the Code and the standard ongoing monitoring procedures and controls established and maintained by each relevant person. Any enhancements to the standard ongoing monitoring will need to be determined by each relevant person relative to the higher ML/FT/PF risk in any particular case and enable the relevant person to manage and mitigate their higher ML/FT/PF risks.

Guidance on ongoing monitoring is at section 3.4.6.

3.8.11 Assessing PEP risk

Code 6

Being identified as a PEP does not automatically mean that an individual must be classed as posing a higher ML/FT/PF risk, nor should such individuals be prejudged as having links to criminal activity or abuse of the financial system. Determining that a client is a PEP and the risks inherent in that PEP status are relevant to the CRA (see section 2.2.9). As with any other customer type, relevant persons should determine whether a particular PEP customer poses a higher risk according to their CRA and their risk appetite per their BRA (see section 2.2.8).

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 ML/FT/PF suspicion.

The FATF's list of indicators/red flags is not an exhaustive list and should be used in conjunction with the other factors to determine the customer risk. Annex 1 of the "FATF Guidance – PEPs, 2013"provides 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 inflated prices.

Other factors may reduce a PEP's risk rating 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. Determinations on the ML/FT/PF risk of PEPs should have a clear rationale and be clearly documented.

3.8.11.1 Interaction of PEP requirements with ECDD requirements

Code 6, 14(5), 15

Where a PEP is assessed as posing a higher risk whether as a result of the initial CRA for a new customer or a review of the CRA for an existing customer, the ECDD requirements under paragraph 15 of the Code must be met in addition to those of paragraph 14.

Guidance on CRAs and risk assessment reviews is in sections 2.2.9 and 2.2.6. Guidance on ECDD is at section 3.4.7.

It is important to appreciate when conducting a CRA or CRA review, that PEP status is one of a number of factors that should be considered when assessing the ML/FT/PF risk posed by the customer, including any mitigating factors. Mitigating factors might include, for example where the service provided is a bank account with a small turnover from expected salary, payments in and debits out to cover household and living expenses, for a PEP in an equivalent jurisdiction.

Code 6(2)

Where a PEP has not been assessed as posing a higher risk of ML/FT/PF they can be treated like any other customer and paragraph 15 of the Code would not apply (though paragraph 14 would continue to apply for foreign PEPs). The reasons for this should be documented as part of recording the CRA in order to be able to demonstrate its basis. The individual must still be identified as a PEP.

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 and ECDD measures set out in the Code should always be applied where relevant, regardless of a detailed knowledge of the PEP.

The below table summarises the requirements in relation to PEPs:

Customer	ECDD (Code 15)	Additional PEP requirements (Code 14(2) – (5))
Higher risk domestic PEP	YES	YES
Standard risk domestic PEP	NO	NO
Higher risk foreign PEP	YES	YES
Standard risk foreign PEP	NO	YES

3.8.12 "Once a PEP, always a PEP"?

Code 3(1)

The definition of a PEP is a natural person who is or has been entrusted with a prominent public function, their family members and close associates.

Relevant persons must determine whether a PEP is still a PEP based on an assessment of risk rather than prescribed time limits. A CRA review would be an appropriate vehicle. Guidance on CRAs and CRA reviews is in sections 2.2.9 and 2.2.6.

In line with FATF Guidance – PEPs, 2013, a default position of "once a PEP, could always remain a PEP" when a PEP is no longer in that prominent public function, should be assumed.

The CRA review should enable the relevant person to determine the risks associated with the PEP when a PEP no longer holds a prominent public function. Particular areas to consider in such an assessment including the jurisdiction(s) concerned, the seniority of the role as well as the individual PEP. Specific considerations could include:

- the nature and duration of the individual's role;
- how much time has passed since they were in the role;
- the level of influence (including 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 PEP's 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.

Relevant persons should be aware that a PEP's 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.

Code 6(2) This risk based approach must 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 higher risk domestic or foreign PEPs. In such circumstances, the CRA should be reviewed to determine whether the relationship still merits ECDD measures.

Code 6(2)(c) If, following a review of the CRA a relevant person determines that an individual should not be treated as a PEP, they should ensure that a clear and detailed rationale explaining this is recorded.

Code 4(2) Subjecting the decision (to change the classification of an individual from PEP to non-PEP status) to a senior management review and approval may assist relevant persons to manage and mitigate their ML/FT/PF risks and ensures consistency in approach.

4. Exemptions and simplified measures

Code Parts 4 and 6
Code para 8(4), 11 (4), (5)

The Code provides certain exemptions from and simplifications to the standard CDD requirements of part 4 of the Code. The majority of these exemptions/simplifications are at Part 6 of the Code, though the Code also provides a timing concession at paragraph 8(4) (see section 3.4.8) and provision for exempted occasional transactions at paragraph 11(4) and (5) which is dealt with in this chapter of the Handbook.

The purpose of these exemptions/simplified measures is to simplify the CDD process and reduce the compliance burden in certain circumstances so that efforts and resources can be focused where they are needed and have most impact.

For clarity, where a customer/underlying client is identified as a PEP, the concessions need only be disapplied if they have been assessed as posing a higher risk.

Code 4 - 6

Use of the concessions is optional and it is for relevant persons (or in the case of the AOBO concession, receiving regulated persons) to make a reasoned determination as to whether they are going to make use of the concession in any particular case. Such determinations must be sensitive to ML/FT/PF risk and mindful of the overarching requirement that the relevant person is able to manage and mitigate their ML/FT/PF risks. The relevant person's risk assessment and CDD procedures are critical in making such decisions. The relevant person should also ensure a record is kept of what concessions are used in what cases. This will assist with their own risk assessments and also aid completion of the Authority's AML/CFT/CPF Statistical Return.

Code 4(2)

Irrespective of the particular exemption/simplified measure a relevant person may use in accordance with any prescribed conditions, relevant persons must always have regard to the overarching requirements of paragraph 4. The procedures and controls for exemptions/simplified measures must be risk sensitive and enable the relevant person to manage and mitigate their ML/FT/PF risks.

In order to use a concession, all of the requirements and conditions of that concession must be met at the outset and on a continuous basis. Where an existing relationship is subsequently found not to meet the concession's conditions, the relevant person must discontinue using the concession.

Code 4(3)

Furthermore, it is the relevant person who is ultimately responsible for ensuring compliance with the Code and other AML/CFT/CPF requirements regardless of any outsourcing or reliance on third parties.

4.1 Exempted occasional transactions

Code 11(4), (5)

The Code provides an exemption from certain verification requirements where occasional transactions fall below certain value thresholds – i.e. they are exempted occasional transactions.

As the exempted occasional transaction provision only applies to transactions (whether single or a series of linked transactions) below certain thresholds, procedures and controls must enable relevant persons to identify linked transactions exceeding the threshold limits so that the exemption is not incorrectly used. It is for relevant persons to determine what are or could be linked transactions according to their risk assessments. Relevant persons should bear in mind that transactions may be linked in ways other than within a particular time period.

Code 3(1)

3 Interpretation

(1) In this Code -

"occasional transaction" means any transaction (whether a single transaction or series of linked transactions, other than a transaction carried out in the course of an established business relationship, formed by a relevant person and for the purposes of this definition, a business relationship is an established business relationship if it is formed by a relevant person where that person has identified, and taken reasonable measures to verify the identity of the person who, in relation to the formation of that business relationship, was the customer;

...

"exempted occasional transaction" means an occasional transaction (whether a single transaction or a series of linked transaction) where the amount of the transaction or, the aggregate in the case of a series of linked transactions, is less in value than –

(a) €5,000 in relation to an activity being undertaken which is included in Class 8(1) (bureau de change) and Class 8(3) (cheque encashment) of the Regulated Activities Order;

(b) €1,000 in relations to an activity being undertaken which is included in Class 8(4) (money transmission services apart from cheque encashment) of the Regulated Activities Order and paragraph 2(6)(r) (~~convertible virtual currency~~Virtual Asset Service Provider) of Schedule 4 to the Proceeds of Crime Act 2008; or

(c) €15,000 in any other case;

Code 11(3), (4), (6)

11 Occasional transactions

(4) Subject to sub-paragraph (6), if the transaction is an exempted occasional transaction the requirements of sub-paragraphs (3)(b) and (c) cease to apply.

Code 11(5), (6), 12(2)(a)

11 Occasional transactions

(5) Subject to sub-paragraph (6), if the transaction is an exempted occasional transaction the requirements of paragraph 12(2)(a)(ii) cease to apply.

Code 12(2), 11(4), (5), 16(2), 18(2)

12 Beneficial ownership and control

(2) A relevant person must, in the case of any customer –

(a) which is not a natural person –

(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;

Code 11(4), (5)

Sub-paragraph 11(4) enables relevant persons to conduct exempted occasional transactions (as specifically defined by the Code) without verifying the identity or legal status of the customer. In addition, where the customer is not a natural person, 11(5) provides that relevant persons conducting exempted occasional transactions do not need to verify the identity of any beneficial owner of the customer.

All other AML/CFT/CPF requirements still apply, including risk assessment and the remaining CDD requirements, ongoing monitoring, sanctions screening and reporting requirements both in respect of the customer and any beneficial owner.

Code 11(6), 15(4)

Use of the exempted occasional transactions measures is conditional on paragraphs 11(6) and 15(4).

Code 11(6), (4), (5)

11 Occasional transactions

(6) Sub-paragraphs (4) and (5) do not apply if –

(a) the customer is assessed as posing a higher risk of ML/FT; or

(b) the relevant person has identified any suspicious activity.

Code 6, 15

Assessing whether a customer poses a higher ML/FT/PF risk is done through the CRA and subsequently, the CRA reviews. Guidance on CRAs is at section 2.2.9.

Code 15, 26, 27

Guidance on ECDD where customers are assessed as higher risk as at section 3.4.7. Guidance on suspicious activity and making internal and external disclosures is at sections 5.3.1 and 5.4.

4.2 Acceptable applicants

4.2.1 The concession

The Code provides an exemption from certain identification and verification requirements where a customer is of a particular category and only acting on its own behalf, such customers are termed “acceptable applicants”.

Code 3(1), 16(3)

3 Interpretation

(1) In this Code -

“acceptable applicant” means a customer in relation to whom the conditions of paragraph 16(3) (acceptable applicants) are met;

The concession is in two parts, the first deals with the customer itself.

Code 16(1), (3), 8(3), 11(3)

16 Acceptable applicants

(1) If each of the conditions in sub-paragraph (3) are met, verification of the identity of a customer is not required to be produced for -

(a) a new business relationship in accordance with paragraph 8(3)(b) and (c); or

(b) an occasional transaction in accordance with paragraph 11(3)(b) and (c)

Code 16(1)

Paragraph 16(1) removes requirements to verify the customer’s identity and legal status. All other AML/CFT/CPF requirements still apply, including risk assessment and the remaining CDD requirements, ongoing monitoring, sanctions screening and reporting requirements.

Code 16(2), (3), 12(2)(a)

16 Acceptable applicants

(2) If each of the conditions in sub-paragraph (3) are met, paragraph 12(2)(a) ceases to apply.

Paragraph 16(2) removes the requirement at paragraph 12(2)(a) for relevant persons to identify and verify the identity of the beneficial owner of a customer that is a non-natural person. All other AML/CFT/CPF requirements still apply.

4.2.2 Conditions for using the concession

Code 16(3)

In order to use the Acceptable applicants concession, all of the requirements and conditions of paragraph 16 must be met at the outset and on a continuous basis. Where an existing relationship is subsequently found not to meet the concession's conditions, the relevant person must discontinue using the concession.

The conditions for using the Acceptable applicants concession are numerous and varied.

4.2.2.1 Which customers may the concession be used for?

Code 16(3)(e), (1), (2)

16 Acceptable applicants

(3) The conditions referred to in sub-paragraphs (1) and (2) are that the relevant person –

(e) is satisfied that –

(i) the customer is acting on its own behalf and not on behalf of a third party; and

(ii) either the customer –

(A) Is a trusted person; or

(B) Is a company listed on a recognised stock exchange or a wholly owned subsidiary of such a company in relation to which the relevant person has taken reasonable measures to establish that there is effective control of the company by an individual, group of individuals or another legal person or legal arrangement (and such persons are treated as beneficial owners for the purposes of this Code).

Code 3(1)

A "trusted person" is a defined term in the Code.

Code 12(2)(b)

As regards being satisfied the customer is acting on its own behalf, the Authority is aware that for administrative purposes, life companies sometimes use policy identifiers when investing funds back to the life company's policyholder liabilities. For the avoidance of doubt, where the life company is the legal and beneficial owner of the funds and the policyholder has not been led to believe that they have rights over the account or investment, the life company is the customer and is

acting on its own behalf. Guidance regarding whether a customer is acting on their own behalf can be found at section 3.4.5.

4.2.2.2 ML/FT/PF risk assessment requirements

Code 16(3)(b), (1), (2)

16 Acceptable applicants

(3) The conditions referred to in sub-paragraphs (1) and (2) are that the relevant person –

(b) has not identified the customer as posing a higher risk of ML/FT;

Code 6, 15, 16(3)(b)

Assessing whether a customer poses a higher ML/FT/PF risk is done through the CRA and CRA reviews. Guidance on CRAs is at section 2.2.9.
Guidance on ECDD where customers are assessed as higher risk as at section 3.4.7.

4.2.2.3 CDD requirements

Code 16(3)(a), (c), (1), (2)

16 Acceptable applicants

(3) The conditions referred to in sub-paragraphs (1) and (2) are that the relevant person –

(a) has identified the customer and has no reason to doubt that identity;

…

(c) knows the nature and intended purpose of the business relationship or occasional transaction;

Code 8(3)(a), 11(3)(a)

The requirement to identify the customer is in accordance with paragraphs 8(3)(a) and 11(3)(a), guidance for which is at section 3.5.

Guidance on the nature and intended purpose of the business relationship or occasional transaction is at section 3.7.

4.2.2.4 Identification of suspicious activity

Code 16(3)(d), (1), (2)

16 Acceptable applicants

(3) The conditions referred to in sub-paragraphs (1) and (2) are that the relevant person –

(d) has not identified any suspicious activity; and

Guidance on suspicious activity and making internal and external disclosures is at sections 5.3.1 and 5.4.

4.3 Persons in a regulated sector acting on behalf of a third party

For ease of reference, the concession is referred to as the "acting on behalf of" or "AOBO" concession.

4.3.1 Definitions

To assist relevant persons to distinguish between the different persons connected with this concession, the following terms will be used throughout this section of the Handbook:

- "receiving regulated person" – is the type of relevant person that is able to use the AOBO concession when receiving a customer;
- "allowed business" – the receiving regulated person's customer that is acting on behalf of another person for whom the AOBO concession is used; and
- "underlying client" – the allowed business's customer that the allowed business is acting on behalf of.

4.3.2 The concession

For a restricted group of regulated persons (receiving regulated persons), the Code provides an exemption from the requirement to look through certain types of customers (allowed businesses) to the customer's underlying clients and the beneficial owners of those underlying clients where the allowed business is acting for another person.

In order to utilise the concession it is for the relevant person to determine whether or not a customer is acting on behalf of another person or persons, and the relevant person should document its rationale in reaching its decision. Guidance at section 3.4.5 of this Handbook can assist with that determination. There may be instances where such an assessment is undertaken, and this paragraph is subsequently deemed not to be applicable.

Code 17(2), 12(2)(b)

17 Persons in a regulated sector acting on behalf of a third party

(2) Where the regulated person determines that a customer is acting on behalf of another person who is an underlying client of the customer (**"underlying client"**), the regulated person need not comply with paragraph 12(2)(b) if each of the following conditions are met -

Code 17(9)

17 Persons in a regulated sector acting on behalf of a third party

(9) In this paragraph "**underlying client**" includes a beneficial owner of that underlying client.

The concession is available whether there is one or a number of underlying clients' and it is available whether underlying clients' funds are segregated or pooled. Irrespective of any pooling of underlying clients' funds, all other AML/CFT/CPF requirements still apply, including risk assessment and CDD requirements (both in respect of the allowed business and as specified for the underlying clients), ongoing monitoring, sanctions screening and reporting requirements. The receiving regulated person must therefore ensure they are able to adhere to these requirements as well as the conditions for using the AOBO concession for each customer and each of the customer's underlying clients.

Code 12(2)(b)

Use of the concession does not mean that funds for higher and standard risk underlying clients cannot be pooled, only that the concession from 12(2)(b) cannot be applied in respect of those higher risk underlying clients. Further where there are higher risks, the Code's enhanced CDD requirements would apply.

4.3.3 Which regulated persons can use the AOBO concession?

Code 17(1) Regulated Activities Order 2011

17 Persons in a regulated sector acting on behalf of a third party

(1) This paragraph only applies to a regulated person holding a licence to carry on regulated activities under -

(a) Class 1 (deposit taking);

(b) Class 2 (investment business);

(c) Class 3 (services to collective investment schemes); or

(d) Class 8 (money transmission services),
of the Regulated Activities Order.

The regulated persons that may use the AOBO concession for their customers are restricted to certain categories licensed under the Financial Services Act 2008. No other categories of regulated person or relevant person may make use of the concession for their customers.

4.3.4 Conditions on using the AOBO concession

Code 17(8), Part 4

17 Persons in a regulated sector acting on behalf of a third party

(8) If the regulated person is unable to comply with any of the provisions of this paragraph, this paragraph ceases to apply and the regulated person must comply with the requirements of Part 4.

In order to use the AOBO concession, all of the requirements and conditions of paragraph 17 of the Code must be met both at the outset and on a continuous basis.

Code 12(2)(b)

Where an existing business relationship is subsequently found to not meet the conditions for making use of the concession, the receiving regulated person must comply with paragraph 12(2)(b) of the Code.

The conditions for using the AOBO concession are numerous and varied.

4.3.4.1 Which customers may the concession be used for?

Code 17(2)(a), (6)

17 Persons in a regulated sector acting on behalf of a third party

(2) … if each of the following conditions are met –

(a) the regulated person is satisfied that the customer is a person specified in sub-paragraph (6)

Code 17(6), (2)(a), Collective Investment Schemes Act 2008, Regulated Activities Order 2011

17 Persons in a regulated sector acting on behalf of a third party

(6) The persons referred to in sub-paragraph (2)(a) are –

(a) a regulated person;

(b) a nominee of a regulated person where the regulated person is responsible for the nominee company's compliance with the AML/CFT legislation;

(c) a collective investment scheme (except for a scheme within the meaning of Schedule 3 (exempt schemes) to the Collective Investment Schemes Act 2008) where the manager or administrator of such a scheme is a regulated person;

(d) where the person referred to in sub-paragraph (2)(a) is an equivalent scheme in a jurisdiction in List C where the manager or administrator of that scheme is a person referred to in head (f);

(e) a designated business;

(f) a person who acts in the course of external regulated business but does not solely carry on activities equivalent to either or both of Class 4 (corporate services) or Class 5 (trust services) under the Regulated Activities Order; and

(g) a nominee company of a person specified in head (f) where that person is responsible for the nominee company's compliance with the AML/CFT requirements at least equivalent to those in this Code.

Code 17(2)(b)

17 Persons in a regulated sector acting on behalf of a third party

(2) … if each of the following conditions are met –

(b) the regulated person is satisfied the customer is regulated and supervised, or monitored for and has measures in place for compliance with, customer due diligence and record keeping requirements in line with FATF Recommendations 10 (Customer Due Diligence) and 11 (Record Keeping);

It is the receiving regulated person's responsibility to ensure that each allowed business is appropriately regulated, supervised or monitored for CDD and record keeping. It is also the receiving regulated person's responsibility to determine whether the allowed business's CDD and record keeping compliance measures are satisfactory per the FATF's Recommendations.

Code4(1), (2), 5, 6

It is for receiving regulated persons to determine, on a case-by-case basis relative to the materiality and risk of ML/FT/PF, how and to what extent they need to go to, to ensure they are satisfied their customer (allowed business) meets these requirements. The receiving regulated person's risk assessments and risk assessment reviews are vital in such determinations.

Code 17(4), (5)

Paragraphs 17(4) and 17(5) of the Code support these requirements and guidance on paragraphs 17(4) and 17(5) is at section 4.3.5.

Other measures include, for example:

- requesting information from the allowed business;
- researching relevant supervisory authorities' websites to verify information obtained from the allowed business;
- reviewing mutual evaluation and follow up reports of the jurisdiction in which the allowed business is operating from; and
- seeking copies of CDD and record keeping procedures from the allowed business.

In order for the AOBO concession to apply on a continuing basis, the customer's allowed business status must continue for as long as the AOBO concession is relied on. Consequently, a receiving regulated person must take measures to ensure it becomes aware of any changes that would affect the customer's allowed business status. This would include changes particular to the customer itself, such as their procedures or regulatory reputation, but it may also include changes to the status of the jurisdiction from which they operate.

Such determinations and the evidence used to make them should be documented and retained in order that the receiving regulated person can demonstrate their rationale and justify their decisions.

Guidance on CRAs and BRAs is at sections 2.2.9 and 2.2.8.
Guidance on CDD, ongoing monitoring and ECDD is in chapter 1.
Guidance on record keeping is at section 6.4.

4.3.4.2 ML/FT/PF risk assessment requirements

Certain risk related requirements are for the receiving regulated person:

Code 17(2)(i)

17 Persons in a regulated sector acting on behalf of a third party

(2) … if each of the following conditions are met –

(i) the customer does not pose a higher risk of ML/FT.

Code 17(2), 6, 15

Assessing whether a customer (allowed business) poses a higher ML/FT/PF risk is done through the CRA and CRA reviews. Guidance on CRAs, including the higher risk factors specified in Code paragraph 15 is at section 2.2.9.

Other risk related requirements are for the customer (allowed business) to do:

Code 17(2)(d), 6

17 Persons in a regulated sector acting on behalf of a third party

(2) … if each of the following conditions are met –

> (d) the customer has risk assessed the underlying client in accordance with paragraph 6 or with AML/CFT requirements at least equivalent to those in this Code and has confirmed to the regulated person that any underlying client in the arrangement does not pose a higher risk;

Code 6, 15

Guidance on CRAs, including the higher risk factors specified in Code paragraph 15 is at section 2.2.9.

Receiving regulated persons must be aware that though the Code prescribes certain required procedures and risk factors for CRAs, the CRA procedures ultimately adopted, ML/FT/PF risk tolerances and categories are unique to the business undertaking the CRA. What an allowed person considers to be standard risk may actually be assessed by the receiving regulated person as posing a higher ML/FT/PF risk.

Code 4(2)

In order to ensure receiving regulated persons are able to manage and mitigate their ML/FT/PF risk, and to minimise the potential for conflict between the receiving regulated person's higher risk customer threshold and that of the allowed business, the receiving regulated person and the allowed business should have a clear understanding of each other's CRA processes and thresholds. Receiving regulated persons should have confidence in the allowed business's CRA procedures such that they are confident that they will not inadvertently take on the underlying clients of their customer without the mitigations that they would consider necessary if that underlying client were taken on by the receiving regulated person direct.

Confirmation from the allowed business to the receiving regulated person should be in writing.

4.3.4.3 CDD requirements

Certain CDD requirements are for both the receiving regulated person and customer (allowed business) to do:

Code 17(2)(e)

> **17 Persons in a regulated sector acting on behalf of a third party**
> (2) … if each of the following conditions are met –
>
> (e) the regulated person and the customer know the nature and intended purpose of the business relationship with the underlying client;

Code 8(1), (3), 11(1), (3)

Guidance on the nature and intended purpose of the business relationship or occasional transaction is at section 3.7.

Some CDD requirements are solely for the customer (allowed business) to do:

Code 17(2)(c), (f), 8 - 12

> **17 Persons in a regulated sector acting on behalf of a third party**
> (2) … if each of the following conditions are met –

(c) the customer has identified and verified the identity of the underlying client in accordance with paragraphs 8 to 12 or with AML/CFT requirements at least equivalent to those in this Code and has no reason to doubt that identity;

…

(f) the customer has taken reasonable measures to establish the source of funds of the underlying client;

Guidance on identifying and verifying identity is at sections 3.5 and 3.6.
Guidance on source of funds is at section 3.8.1.

4.3.4.4 Identification of suspicious activity

The Code places the onus on both the receiving regulated person and the customer (allowed business) in respect of suspicious activity and ceasing use of the AOBO concession:

Code 17(2)(g)

17 Persons in a regulated sector acting on behalf of a third party

(2) … if each of the following conditions are met –

(g) neither the regulated person nor the customer has identified any suspicious activity;

Code 17(7)

17 Persons in a regulated sector acting on behalf of a third party

(7) If suspicious activity is identified this paragraph ceases to apply and an internal disclosure must be made.

Code 26, 27

This requirement should be read in the broadest sense in relation to the parties involved in the business relationship/occasional transaction. Guidance on suspicious activity and making internal and external disclosures is at sections 5.3.1 and 5.4.

4.3.4.5 Written terms of business

Code 17(2)(h)

17 Persons in a regulated sector acting on behalf of a third party

(2) … if each of the following conditions are met –

(h) written terms of business are in place between the regulated person and the customer in accordance with sub-paragraph (3);

It is a matter for the regulated person to decide the form the written terms of business will take. For example, in some cases it may be appropriate for a written terms of business to be entered into for each individual business relationship. Alternatively, for example where an allowed business acts on behalf of several underlying clients, relevant persons may find it more helpful to have a centralised written terms of business which is linked to the relevant files on the underlying clients.

However, the written terms of business requirement is satisfied, relevant persons must be able to relate the terms of business to the relevant underlying clients and vice versa on an ongoing basis.

Code 17(3)

The written terms of business must comply with paragraph 17(3).

Code 17(3)(a), (6)

17 Persons in a regulated sector acting on behalf of a third party

(3) The written terms of business referred to in sub-paragraph (2)(h) must require the customer to –

(a) supply to the regulated person information concerning the identity of any underlying client –

(i) in the case of a customer to whom sub-paragraph (6)(a), (b), (c) or (e) applies, on request; and

(ii) in relation to a customer to who sub-paragraph 6(d), (f) or (g) applies, immediately;

Though the concession means the receiving regulated person does not have to identify the underlying client itself, the customer (allowed business) must supply identity information to the receiving regulated person either at the outset of the business relationship or on request (depending on the type of allowed business).

Guidance on identity information is at section 3.5.

Code 17 (3)(b), (2)(h)

17 Persons in a regulated sector acting on behalf of a third party

(3) The written terms of business referred to in sub-paragraph (2)(h) must require the customer to –

(b) supply to the regulated person immediately on request copies of the documents, data or information used to verify the identity of the underlying client and all other due diligence information held by the customer in respect of the underlying client in any particular case;

Receiving regulated persons and their allowed businesses customers should note that in addition to verification of identity documents, data or information, this requirement includes all other CDD information including CDD documents and data.

Guidance on CDD is in chapter 1.
Guidance on verification of identity is at section 3.6.

Code 17(4), 17(2)(b), 17(5)

There are many circumstances when regulated persons may request copies of documents, data or information used to verify identity or any other CDD information which includes where:

- the regulated person wishes to satisfy itself that the allowed business's CDD and record keeping procedures are fit for purpose;
- the regulated person is testing the effectiveness of the procedures;
- the regulated person considers it necessary to obtain such documents, data or information as part of ongoing monitoring procedures, sanctions screening or in relation to unusual or potentially suspicious activity; and/or
- the regulated person is complying with, for example, requests for information or other enquiries from competent authorities.

This list is not exhaustive.

Code 17(3)(c), (2)(h)

17 Persons in a regulated sector acting on behalf of a third party

(3) The written terms of business referred to in sub-paragraph (2)(h) must require the customer to –

(c) confirm to the regulated person that the arrangement does not involve an underlying client in the arrangement who has been assessed as higher risk by the customer;

Code 17(2)(d)

This confirmation concerns the requirement at paragraph 17(2)(d) of the Code. Guidance for paragraph 17(2)(d) is at section 4.3.4.2.

Code 17(3)(d), (2)(h)

17 Persons in a regulated sector acting on behalf of a third party

(3) The written terms of business referred to in sub-paragraph (2)(h) must require the customer to –

(d) inform the regulated person specifically of each case where the customer is not required or has been unable to verify the identity of an underlying client;

This term is relevant both at the outset of the business relationship/occasional transaction and to any changes in identity information as the business relationship progresses.

Code 12

For example, this term would apply where there are changes to specific pieces of identity information previously obtained such as the name or address of an underlying client. It would also apply where there is a change in the beneficial ownership or control of the underlying client in accordance with paragraph 12 of the Code.

Guidance on change of CDD information is at section 3.3.6.

Code 17(3)(e), (2)(h)

17 Persons in a regulated sector acting on behalf of a third party

(3) The written terms of business referred to in sub-paragraph (2)(h) must require the customer to –

(e) inform the regulated person if the customer is no longer able to comply with the provisions of the written terms of business because of a change of the law applicable to the customer; and

This might include, for example, where there are changes to the secrecy laws in the customer's (allowed business) jurisdiction.

Code 17(3)(f), (2)(h)

17 Persons in a regulated sector acting on behalf of a third party

(3) The written terms of business referred to in sub-paragraph (2)(h) must require the customer to –

(f) do all things as may be required by the regulated person to enable the regulated person to comply with its obligations under sub-paragraph (2).

Code 17(2), (4)

This is relevant to both paragraphs 17(2) and 17(4) which is a specific requirement pertaining to paragraph 17(2).

4.3.5 Ensuring appropriate and effective AOBO procedures

Code 17(4), (2)

17 Persons in a regulated sector acting on behalf of a third party

(4) In satisfying the conditions of sub-paragraph (2), the regulated person must take reasonable measures to ensure that –

(a) the documents, data or information supplied or to be supplied are satisfactory; and

(b) the customer due diligence procedures and controls of the customer are fit for purpose.

Code 17

The purpose of this requirement is to ensure that all the procedures established under paragraph 17, both by the receiving regulated person and the customer (allowed business) are appropriate from the outset of any AOBO business and going forward for the necessary duration.

Code 17(2), (3)

It is the receiving regulated person's responsibility to ensure compliance with the concession's conditions, including those conditions that are for the customer (allowed business) to do. The receiving regulated person must also ensure that, as far as they can reasonably determine, the written terms of business will be complied with in full by the allowed business at all times. This includes being able to obtain satisfactory identity verification documents, data or information as well as any other CDD information from the customer (allowed business) as soon as the receiving regulated person requests it.

This means the regulated person must be satisfied that the allowed business's verification of identity and other CDD procedures, record keeping and retention

procedures are satisfactory, both at the outset of any AOBO business and on an ongoing basis.

Regulated persons should also consider the allowed business's procedures for supplying verification of identity documents, data and information and other CDD information to the regulated person to ensure that the regulated person's needs are part of the allowed business's procedures.

Code 4(1), (2), 5, 6

It is for receiving regulated persons to determine, on a case-by-case basis relative to the materiality and risk of ML/FT/PF, how and to what extent they need to go to, to ensure the procedures are satisfactory and remain so. The receiving regulated person's risk assessments and risk assessment reviews are vital in such determinations. Measures receiving regulated persons could adopt include, for example:

- providing the allowed business with information on the regulated person's own expectations for methods to be used to verify identity, record keeping and for wider CDD requirements;
- reviewing the allowed business's verification of identity, record keeping and supply procedures to ensure they are satisfactory;
- requesting details of any changes to such procedures;
- requesting copies of an independent review of the allowed business's procedures by an external auditor or other experts;
- making enquiries as to the allowed business's reputation and regulatory track record, and the extent to which any group standards are applied and audited; and/or
- visits to allowed businesses to gain an in depth understanding of the allowed business's procedures.

Code 17(8)

Where either the receiving regulated person's or the customer's (allowed business's) AOBO procedures are not satisfactory, the AOBO concession must not be used.

Code 17(5)

17 Persons in a regulated sector acting on behalf of a third party

(5) The regulated person must take reasonable measures to satisfy itself that –

(a) the procedures for implementing this paragraph are effective by testing them on a random and periodic basis at least once every 12 months; and

(b) the written terms of business confer the necessary rights required by this paragraph on the regulated person.

Code 17

The purpose of this requirement is to ensure that, in practice, the procedures established under paragraph 17, both by receiving regulated person and the customer (allowed business) are effective.

In respect of testing the receiving regulated person's own procedures this includes procedures for:

Code 6, 17(2)(i)
Code 17(2)
Code 17(2), (3)
Code 17(3)(a), 17(2)(e)
Code 17(2)(g), (7)
Code 17(8)

- CRAs on allowed businesses;
- conducting due diligence on the customer to ensure it is eligible to be an allowed business;
- entering into and ensuring satisfactory terms of business;
- CDD measures on the underlying client for which the receiving regulated person retains responsibility for example obtaining identity information and information on the nature and intended purpose of the business relationship with the underlying client;
- identifying and dealing with suspicious activity; and
- stopping use of the AOBO concession where the Code's provisions cannot be met.

Code 30

There may be some crossover with the requirements of paragraph 30 of the Code. Guidance on monitoring and testing as required by paragraph 30 is at section 6.1.

As regards testing the allowed business's procedures this includes their procedures for:

Code 17(2)(b)-(f), 17(3)(a), (b)
Code 17(3)(a), (f)
Code 17(2)(d), 17(3)(c)
Code 17(2)(g)
Code 17(3)(d), (e)

- CDD and record keeping in respect of the underlying clients and beneficial owners of the underlying clients;
- supplying identity information, verification of identity and other CDD information to the receiving regulated person;
- CRAs, including their thresholds and parameters for higher risk business;
- identifying and dealing with suspicious activity; and
- communicating with the receiving regulated person where the allowed business is not required or unable to verify identity of an underlying client (including any beneficial owner of an underlying client), or where the allowed business cannot comply with the terms of business.

It is for receiving regulated persons to determine, on a case-by-case basis relative to the materiality and risk of ML/FT/PF, the most appropriate methods to test that the procedures are satisfactory. Possible methods to test the allowed business's procedures include, for example:

- requesting copies of the verification or identity documents, data or information and on a sample of underlying clients;
- requesting other CDD information held by the allowed business on a sample of underlying clients;

- seeking other evidence that the allowed business is complying with the record keeping requirements in line with the FATF Recommendations;
- requesting copies of the allowed business's CRA for a sample of underlying clients;
- seeking confirmation of any cases where the allowed business is not required or has been unable to verify an underlying client's identity or the identity of an underlying client's beneficial owner; and
- reviewing relevant legislation in the allowed business's jurisdiction to establish if there has been a change in the law meaning the allowed business is no longer able to comply with the terms of business.

This list is not exhaustive.

Code 17(5)(a), 4(2), (6)

In accordance with the risk based approach, the frequency (subject to the 12 month specified minimum) and extent of any such testing is for the receiving regulated person to determine in accordance with the outcomes of the CRA. Whatever the extent, methods used and the frequency of testing a receiving regulated person determines is appropriate, receiving regulated persons must always have regard to the overarching requirement to ensure they are able to manage and mitigate their ML/FT/PF risks.

4.4 Generic designated business

4.4.1 The Concession

The Code provides an exemption from certain verification requirements where a relevant person is conducting generic designated business.

The concession is in two parts. The first deals with the customer itself.

Code 18(1), (3), 8(3)(b), (c), 11(3)(b), (c)

18 Generic designated business

(1) If each of the conditions in sub-paragraph (3) are met and the relevant person is conducting generic designated business, verification of the identity of a customer is not required to be produced for-

(a) a new business relationship in accordance with paragraph 8(3)(b) and (c); or

(b) an occasional transaction in accordance with 11(3)(b) and (c).

Code 18(1)

Paragraph 18(1) therefore disapplies verification of the customer's identity and legal status requirements. All other AML/CFT/CPF requirements still apply, including risk assessment and the remaining CDD requirements, ongoing monitoring, sanctions screening and reporting requirements.

The second deals with the beneficial owner.

Code 18(2), 12(2)(a)(ii)

18 Generic designated business

(2) If each of the conditions in sub-paragraph (3) are met paragraph 12(2)(a)(ii) ceases to apply.

Code 18(2)

Paragraph 18(2) removes the requirement to verify the identity of the beneficial owner of a customer that is a non-natural person. All other AML/CFT/CPF requirements still apply.

4.4.2 What is generic designated business?

Code 18(4)

18 Generic designated business

(4) In this paragraph –

"generic designated business" for the purpose of this paragraph means designated business carried on by a relevant person where the relevant person –

(a) does not participate in financial transactions on behalf of a customer; and

(b) does not administer or manage a customer's funds, with its own funds or other customer's funds, on a pooled bank account basis.

Code 3(1)

3 Interpretation

(1) In this Code -
"designated business" mean a person that is registered by the Isle of Man Financial Services Authority to undertake designated business listed in Schedule 1 to the Designated Businesses (Registration and Oversight) Act 2015;

It will be primarily accountants and tax advisers that can avail themselves of the generic designated business concession. This is because they often advise on aspects of a financial transaction rather than directly participating in the transaction. Examples of the types of services that would fall within the definition of generic designated business include:

- preparing and issuing management accounts or statutory financial statements;
- preparing and issuing audit reports;
- book keeping services;
- providing tax advice to customers; and
- completing annual tax return on behalf of customers.

4.4.3 Conditions for using the concession

Code 8, 11, 12

If the conditions are not met, the generic designated business concession must not be used and full verification must be obtained per paragraphs 8, 11 and 12.

4.4.3.1 ML/FT/PF risk assessment requirements

Code 18(3)(b), (1), (2)

18 Generic designated business

(3) The conditions referred to in sub-paragraphs (1) and (2) are that the relevant person –

(b) has not identified the customer as posing a higher risk of ML/FT;

Code 6, 15, 18(3)(b)

Assessing whether a customer poses a higher ML/FT/PF risk is done through the CRA and CRA reviews. Guidance on CRAs is at section 2.2.9.

Code 15

Guidance on ECDD where customers are assessed as higher risk as at section 3.4.7.

4.4.3.2 CDD requirements

Code 18(3)(a), (c), (e) 8(3)(e)

18 Generic designated business

(3) The conditions referred to in sub-paragraphs (1) and (2) are that the relevant person –

(a) has identified the customer and has no reason to doubt that identity;

…

(c) knows the nature and intended purpose of the business relationship or occasional transaction;

…

(e) has taken reasonable measures to establish the source of funds in accordance with paragraph 8(3)(e).

Code 18(3)(a), 8(3)(a), 11(3)(a)

The requirement to identify the customer is in accordance with paragraphs 8(3)(a) and 11(3)(a), guidance for which is at section 3.5.

Code 18(3)(c), (e)

Guidance on the nature and intended purpose of the business relationship or occasional transaction is at section 3.7.
Guidance on establishing source of funds is at section 3.8.2.

4.4.3.3 Identification of suspicious activity

Code 18(3)(d), (1), (2)

18 Generic designated business

(3) The conditions referred to in sub-paragraphs (1) and (2) are that the relevant person –

(d) has not identified any suspicious activity;

Guidance on suspicious activity and making internal and external disclosures is at sections 5.3.1 and 5.4.

4.5 Eligible introducers

Code 3(1), 19

3 Interpretation

(1) In this Code -
"eligible introducer" refers to a person ("**the eligible introducer**") who introduces a customer to a relevant person under the circumstances covered in paragraph 19

(eligible introducer). It includes situations where reliance, in relation to verification of a customer's identity, is placed on the eligible introducer. The verification is not required to be produced to the relevant person if the conditions in paragraph 19 are satisfied;

The Code allows relevant persons to rely on certain third parties, termed eligible introducers, to undertake and hold verification of identity on the customers they introduce to the relevant person and the beneficial owners of those customers. The relevant person can rely on the eligible introducer to retain the verification of identity documents, data or information without passing it on to the relevant person at the outset of the business relationship/occasional transaction.

All other AML/CFT/CPF requirements still apply, including risk assessment and the remaining CDD requirements, ongoing monitoring, sanctions screening and reporting requirements.

Relevant persons must note that the eligible introducer provisions are not the same as the requirements regarding introduced business which are explained at section 3.4.3.

Code 19(12)

19 Eligible introducers

(12) The ultimate responsibility for ensuring that procedures comply with the terms of the Code remains with the relevant person and not with the eligible introducer.

Whatever reliance relevant persons place on eligible introducers, the relevant person is ultimately responsible.

Code 19(1), (4), (5), 9, 8, 11

19 Eligible introducers

(1) If a customer is introduced to a relevant person by a third party, other than an introducer to which paragraph 9 applies, the relevant person may, if it thinks fit, comply with this paragraph, instead of paragraphs 8 or 11 provided -

(a) the eligible introducer agrees to the relevant person doing so; and

(b) each of the conditions in sub-paragraphs (4) and (5) are met.

It is a matter for relevant persons to make a reasoned determination as to whether they believe it is appropriate to follow the requirements of paragraph 19 rather than those of paragraph 8 or 11 in any particular case. Such determinations must be sensitive to ML/FT/PF risk and ensure that whatever procedures are followed, the relevant person is able to manage and mitigate their ML/FT/PF risks. The relevant person's risk assessments are critical in making such determinations.

Code 19(6), (7)

Eligible introducers must actively agree to reliance being placed on them, and this should be appropriately recorded. Paragraphs 19(6) and (7) require a written terms of business to be in place between the relevant person and the eligible

introducer before any eligibly introduced business relationship is entered into. Guidance on the written terms of business is at section 4.5.1.7.

4.5.1 Conditions on using the eligible introducer concession

Conditions for using the eligible introducer concession are numerous and varied.

4.5.1.1 Timing for completing eligible introducer concession conditions

Code 19(3)

> **19 Eligible introducers**
>
> (3) The procedures and controls of this paragraph must be undertaken before a business relationship or occasional transaction is entered into.

Code 8, 11, 19

Where relevant persons choose to comply with paragraph 19 rather than paragraph 8 or 11, there is no timing concession available.

4.5.1.2 Persons that can be eligible introducers

Code 19(4)(f), (g), (5)

> **19 Eligible introducers**
>
> (4) Verification of a customer's identity is not required to be produced by the eligible introducer if the relevant person –
>
> (f) is satisfied that –
>
> (i) the eligible introducer is a trusted person other than a nominee company of either a regulated person or a person who acts in the course of external regulated business; or
>
> (ii) each of the conditions in sub-paragraph (5) are met; and
>
> (g) has conducted a risk assessment of the eligible introducer and is satisfied that the eligible introducer does not pose a higher risk or ML/FT.

Code 19(5), (4)(f), 33 - 37, Parts 4, 5

> **19 Eligible introducers**
>
> (5) The conditions referred to in sub-paragraph 4(f)(ii) are that –
>
> (a) the relevant person and the eligible introducer are bodies corporate in the same group;
>
> (b) the group operates AML/CFT programmes and procedures which conform to Parts 4 and 5 and paragraphs 33 to 37;
>
> (c) the operation of those programmes and procedures is supervised at a group level by an appropriate authority; and
>
> (d) the group's AML/CFT policies adequately mitigate any risk associated with a jurisdiction for the time being specified on List A or List B.

Code 19(4), (5), 15, 3(1)

Eligible introducers can either be a restricted category of "trusted persons" as defined in the Code, or group companies subject to listed conditions. Whether

they are trusted persons or group entities, eligible introducers must not pose a higher ML/FT/PF risk.

Guidance on eligible introducer risk assessments is below at section 4.5.1.4.

Code 4(1), (2)

It is for relevant persons to determine how and the extent they need to go to, to ensure they are satisfied of the introducer's eligibility on a case-by-case basis relative to the materiality and risk of ML/FT/PF. Relevant persons should establish their own lists of the source documents, data and information they will use to determine whether an introducer is a (restricted) trusted person bearing in mind the principles and considerations set out in chapter 1 of the Handbook on reliability and the relevant person's risk assessments. Such lists should be maintained and reviewed to ensure they continue to be appropriate per the risk assessments and any reviews of these risk assessments.

Code 4(3), 19(5), (12)

It is also a relevant person's responsibility to ensure that before reliance is place on a group company, the relevant person is satisfied that all the conditions at paragraph 19(5) are satisfied. Relevant persons must be able to demonstrate this is the case, before accepting business from a group entity under the eligible introducer provisions.
Guidance on CDD, ongoing monitoring and enhanced CDD is in chapter 1.
Guidance on Code paragraphs 33 to 37 is in chapters 6 and 1.

Code 19(10)(b)

19 Eligible introducers

(10) In order to rely on an eligible introducer a relevant person must –

(b) take such measures as necessary to ensure it becomes aware of any material change to the eligible introducer's status or the status of the jurisdiction in which the eligible introducer is regulated.

Code 4, 13(1), 19(10)

Being satisfied of the eligibility of introducers is a requirement both at the outset of the business relationship/occasional transaction and an ongoing requirement, for as long as the relevant person places reliance on the eligible introducer. Should the introducer no longer be eligible the eligible introducer concession must no longer be used.

Code 4(2)

The steps taken must enable the relevant person to manage and mitigate their ML/FT/PF risks.

4.5.1.3 No reliance by the eligible introducer

Code 19(10)(a)

19 Eligible introducers

(10) In order to rely on an eligible introducer a relevant person must –

(a) take measures to satisfy itself that the eligible introducer is not itself reliant on a third party for the verification of identity of the customer; and

Chains of reliance are not permissible. This requirement is relevant both at the outset of any eligibly introduced business relationship/occasional transaction, and for the duration reliance is place on the eligible introducer.

4.5.1.4 Customer and eligible introducer ML/FT/PF risk assessment requirements

Code 19(2), 6

19 Eligible introducers

(2) The relevant person must establish, maintain and operate customer risk assessment procedures in accordance with paragraph 6.

As emphasised at paragraph 19(2), the CRA requirements still apply.

Code 19(4)(b), (g)

19 Eligible introducers

(4) Verification of a customer's identity is not required to be produced by the eligible introducer if the relevant person –

(b) has not identified the customer as posing a higher risk of ML/FT;

…

(g) has conducted a risk assessment of the eligible introducer and is satisfied that the eligible introducer does not pose a higher risk or ML/FT.

Code 19(4)(b), 19(2), 6, 15

Assessing whether a customer poses a higher ML/FT/PF risk is done through the CRA and CRA reviews. Guidance on CRAs, including the higher risk factors specified in Code paragraph 15 is at section 2.2.9.

Code 15

Guidance on ECDD where customers are assessed as higher risk as at section 3.4.7.

Code 19(4)(g), 6(3)(e)

Paragraph 19(4)(g) also requires relevant persons to conduct a risk assessment of the eligible introducer. The guidance on risk assessments at section 2.2 should be used to assist relevant persons in establishing, recording, operating and maintaining their eligible introducer risk assessment procedures and controls. The specific guidance on the Code 6(3)(e) risk factor (the involvement of any third parties for elements of the CDD process) is particularly pertinent for determining whether an eligible introducer poses a higher ML/FT/PF risk. See section 2.2.9.2 .

How a relevant person chooses to organise their eligible introducer risk assessments should be determined on a case-by-case basis. For example, in some cases it may be appropriate for the eligible introducer risk assessment to be documented as part of the relevant CRA. Alternatively, for example where an eligible introducer has introduced several customers, relevant persons may find it more helpful to have a centralised eligible introducer risk assessment file which is linked to the relevant customer files. If a relevant person chooses to complete centralised eligible introducer risk assessments these do not need to be updated every time a piece of new business is received from that eligible introducer. However, every eligibly introduced business relationship/occasional transaction must include consideration of the eligible introducer risk assessment (e.g. whether

the piece of business received from the eligible introducer is in line with expected business from that eligible introducer).

Whatever system of organisation is used, relevant persons must be able to relate the eligible introducer risk assessment to the relevant customers and vice versa on an ongoing basis.

4.5.1.5 CDD requirements

Code 19(4)(a), (c), (d) 8(3)(e)

19 Eligible introducers

(4) Verification of a customer's identity is not required to be produced by the eligible introducer if the relevant person –

(a) has identified the customer and any beneficial owner and has no reason to doubt those identities;

…

(c) knows the nature and intended purpose of the business relationship;

(d) has taken reasonable steps to establish the source of funds including the measures specified in paragraph 8(3)(e);

Code 19, 8, 9, 11

Paragraph 19 replaces paragraphs 8 and 11, consequently the paragraph 19 CDD requirements apply instead of those at paragraphs 8 and 11. The concession itself is only from verification of identity. All other CDD requirements listed at paragraph 19 or in Code paragraphs other than 8, 9 and 11 apply.

Code 12

In respect of beneficial ownership and control requirements at paragraph 12, all the requirements will apply except requirements to take reasonable measures to verify identity. For example, relevant persons must still determine whether the customer is acting on behalf of another person and if so, identify that other person per paragraph 12(2)(b)(i). But relevant persons could place reliance on the eligible introducer for verifying that other person's identity under 12(2)(b)(ii).

Code 19(4)(a)

Guidance on beneficial ownership and control is at section 3.4.5.
Guidance on identifying customers and beneficial owners is at section 3.5.
Guidance on the nature and intended purpose of the business relationship or occasional transaction is at section 3.7.
Guidance on source of funds is at section 3.8.1.

4.5.1.6 Identification of suspicious activity

Code 19(4)(e)

19 Eligible introducers

(4) Verification of a customer's identity is not required to be produced by the eligible introducer if the relevant person –

(e) has not identified any suspicious activity;

Code 26, 27

Guidance on suspicious activity and making internal and external disclosures is in chapter 5.

4.5.1.7 Written terms of business

Code 19(6)

19 Eligible introducers

(6) The relevant person must not enter into a business relationship with a customer that is introduced by an eligible introducer unless written terms of business are in place between the relevant person and the eligible introducer

It is a matter for relevant persons to decide the form the written terms of business will take. For example, in some cases it may be appropriate for a written terms of business to be entered into for each individual business relationship. Alternatively, for example where an eligible introducer has introduced several customers, relevant persons may find it more helpful to have a centralised written terms of business which is linked to the relevant customer files.

However, the written terms of business requirement is satisfied, relevant persons must be able to relate the terms of business to the relevant customers and vice versa on an ongoing basis.

Code 19(7)

The written terms of business must comply with paragraph 19(7).

Code 19(7)(a)(b), (4), (5), 8 - 12

19 Eligible introducers

(7) Without limiting sub-paragraphs (4) and (5), those terms of business must require the eligible introducer to –

(a) verify the identity of all customers introduced to the relevant person in accordance with paragraphs 8 to 12 or with AML/CFT requirements at least equivalent to those in this Code and has no reason to doubt those identities;

(b) take reasonable measures to verify the identity of any beneficial owners in accordance with paragraphs 8 to 12 or with AML/CFT requirements at least equivalent to those in this Code and has no reason to doubt those identities;

Guidance on verification of identity requirements is at section 3.6.

Code 19(7)(e), (4), (5)

19 Eligible introducers

(7) Without limiting sub-paragraphs (4) and (5), those terms of business must require the eligible introducer to –

(e) supply to the relevant person immediately on request, copies of the documents, data or information used to verify the identity of the customer

and any beneficial owner and all other customer due diligence information held by the eligible introducer in any case;

Relevant persons and eligible introducers should note that this requirement covers documents, data or information wider in scope than solely the verification of identity documents, data or information for which the relevant person is placing reliance on the eligible introducer.

Guidance on CDD is in chapter 1.
Guidance on verification of identity is at section 3.6.

There are many circumstances when relevant persons may request copies of documents, data or information used to verify identity or any other CDD information which include where:

Code 19(8)

Code 19(9)

Code 19(10)

- the relevant person wishes to satisfy itself that the eligible introducer's procedures are fit for purpose;
- the relevant person is testing the effectiveness of the procedures;
- the relevant person is satisfying itself that the eligible introducer does not rely on a third party;
- the relevant person considers it necessary to obtain such documents, data or information as part of ongoing monitoring procedures, sanctions screening or in relation to unusual/suspicious activities; and/or
- the relevant person is complying with for example requests for information or other enquiries from competent authorities.

This list is not exhaustive.

Code 19(7)(f), (4), (5)

19 Eligible introducers

(7) Without limiting sub-paragraphs (4) and (5), those terms of business must require the eligible introducer to –

(f) supply to the relevant person immediately copies of the documents, data or information used to verify the identity of the customer and any beneficial owner and all other customer due diligence information, held by the eligible introducer in any particular case if –

(i) the eligible introducer is to cease trading;

(ii) the eligible introducer is to cease doing business with the customer;

(iii) the relevant person informs the eligible introducer that it no longer intends to rely on the terms of business referred to in this paragraph; or

(iv) the eligible introducer informs the relevant person that it no longer intends to comply with the terms of business referred to in this paragraph;

Relevant persons and eligible introducers should note that this requirement covers documents, data or information wider in scope than solely the verification of identity documents, data or information for which the relevant person is placing reliance on the eligible introducer.

Code 19(7)(g), (4), (5)

19 Eligible introducers

(7) Without limiting sub-paragraphs (4) and (5), those terms of business must require the eligible introducer to –

(g) inform the relevant person specifically of each case where the eligible introducer is not required or has been unable to verify the identity of the customer or any beneficial owner within a reasonable timeframe; and in such a case –

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

(ii) the relevant person must consider terminating that business relationship; and

(iii) the relevant person must consider making an internal disclosure in relation to that business relationship or occasional transaction;

This term is relevant both at the outset of the business relationship/occasional transaction and to any changes in identity information as the business relationship progresses.

Code 10, 12

For example, this term would apply where there are changes to specific pieces of identity information previously obtained such as name or address. It would also apply 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 or control of a customer in accordance with paragraph 12 of the Code.

Guidance on change of CDD information is at section 3.3.6.

Code 19(7)(h), (4), (5)

19 Eligible introducers

(7) Without limiting sub-paragraphs (4) and (5), those terms of business must require the eligible introducer to –

(h) inform the relevant person if the eligible introducer is no longer able to comply with the provisions of the written terms of business because of a change of the law applicable to the eligible introducer; and

This might include, for example, where there are changes to the secrecy laws in the eligible introducer's jurisdiction.

Code 19(7)(i), (4), (5), (9)

19 Eligible introducers

(7) Without limiting sub-paragraphs (4) and (5), those terms of business must require the eligible introducer to –

(i) do all such things as may be required by the relevant person to enable the relevant person to comply with its obligation under sub-paragraph (9).

Code 19(9)(b)

19 Eligible introducers

(9) A relevant person must take measures to satisfy itself that –

(b) the written terms of business confer the necessary rights on the relevant person to satisfy the requirements of this paragraph.

Code 19(9)

19(9) concerns relevant persons ensuring the effectiveness of the procedures required by paragraph 19 by testing them. It also emphasises that the terms of business must confer the necessary rights on the relevant person.

4.5.2 Ensuring appropriate and effective eligible introducer procedures

Ensuring appropriate and effective eligible introducer procedures involves both the procedures themselves as well as testing that the procedures are effectively implemented.

Code 19(8)

19 Eligible introducers

(8) A relevant person must ensure that the procedures under this paragraph are fit for the purpose of ensuring that the documents, data or information used to verify the identity of the customer and any beneficial owner are satisfactory and that the procedures of the eligible introducer are likewise fit for that purpose.

Code 19

The purpose of this requirement is to ensure that all the procedures established in respect of paragraph 19, both by the relevant person and the eligible introducer are appropriate both from the outset of any eligibly introduced business and going forward for the necessary duration. The relevant person must be able to obtain satisfactory identity verification documents, data or information from the eligible introducer.

Even where relevant persons place reliance on an eligible introducer to obtain and hold identity verification documents, data and information, it remains the relevant person's responsibility to ensure that the documents, data or information will (according to their own procedures and the requirements of the Code) be satisfactory and will be provided to the relevant person should the need arise.

This means the relevant person must be satisfied that the eligible introducer's verification of identity, record keeping and retention procedures are satisfactory, both when eligible introductions are made and on an ongoing basis.

Relevant persons should also consider the eligible introducers' procedures for supplying verification of identity documents, data and information to the relevant person to ensure that the relevant person's needs are part of the eligible introducer's procedures should any of the trigger events for supplying the verification of identity to the relevant person occur.

It is for relevant persons to determine how they will ensure the procedures are satisfactory and remain so. Some possible examples could include:

- providing the eligible introducer with information on the relevant person's own expectations for methods to be used to verify identity and record keeping;
- reviewing the eligible introducer's verification of identity, record keeping and supply procedures to ensure they are satisfactory; requesting details of any changes to such procedures;
- requesting copies of an independent review of the eligible introducer's procedures by an external auditor or other experts;
- making enquiries as to the eligible introducer's reputation and regulatory track record, and the extent to which any group standards are applied and audited; and
- visits to eligible introducers to gain an in depth understanding of the eligible introducer's procedures.

The eligible introducer and CRAs are vital in determining the most appropriate approach and ensuring the documents, data and information are satisfactory in any particular case.

Code 19(9)

19 Eligible introducers

(9) A relevant person must take measures to satisfy itself that –

(a) the procedures for implementing this paragraph are effective by testing them on a random and periodic basis at least once every 12 months; and

(b) the written terms of business confer the necessary rights on the relevant person to satisfy the requirements of this paragraph.

Code 19

The purpose of this requirement is to ensure that, in practice, the procedures established for paragraph 19, both by the relevant person and the eligible introducer are effective. It is for relevant persons to determine, on a case-by-case basis relative to the materiality and risk of ML/FT/PF, the most appropriate methods to test that the procedures are satisfactory.

In respect of testing the relevant person's own procedures this includes procedures for:

Code 19(4)

- risk assessing the eligible introducer;

Code 19(4), (5), (10)
Code 19(1), (6), (7)
Code 19(2), (4)
Code 19(7)(g), (11)

- conducting due diligence on the introducer to ensure eligibility and that they are not themselves reliant on a third party;
- entering into and ensuring satisfactory terms of business;
- conducting CRA and the remaining CDD requirements; and
- ensuring requirements for stopping and or terminating business relationships/occasional transactions and making internal disclosure are met.

Code 30

There may be some crossover with the requirements of paragraph 30.

Guidance on monitoring and testing as required by paragraph 30 is at section 6.1.

As regards testing the eligible introducer's procedures this includes their procedures for:

Code 19(7)(a), (b)
Code 19(7)(e), (f)
Code 19(7)(c), (d)
Code 19(7)(e), (f)

- verification of identity both of customers and beneficial owners;
- other CDD information;
- record keeping and retention both in respect of CDD and transaction records relevant to the eligibly introduced customers;
- supplying verification of identity and other CDD information to the relevant person; and
- communication with the relevant person where the eligible introducer is not required or unable to verify identity, or where the eligible introducer cannot comply with the terms of business.

Possible examples could include (but are not limited to):

- requesting copies of the verification or identity documents, data or information on a sample of customers;
- requesting other CDD information held by the eligible introducer on a sample of customers;
- requesting copies of the transaction records between the eligible introducer and the customer where the records are concerned with or arise out of the introduction on a sample of customers;
- seeking other evidence that the eligible introducer is complying with the record keeping requirements of the terms of business;
- seeking confirmation of any cases where the eligible introducer is not required or has been unable to verify a customer or beneficial owner's identity; and
- reviewing relevant legislation in the eligible introducer's jurisdiction to establish if there has been a change in the law meaning the eligible introducer is no longer able to comply with the terms of business.

Code 4(2)

In accordance with the risk based approach, the frequency (subject to the 12 month specified minimum) and extent of any such testing is for the relevant person to determine in accordance with the outcomes of the CRAs and the eligible introducer risk assessments. Whatever the extent, methods used and the frequency of testing a relevant person determines is appropriate, relevant persons must always have regard to the overarching requirement to ensure they are able to manage and mitigate their ML/FT/PF risks.

4.5.3 Unable to meet eligible introducer requirements

Code 19(11)

19 Eligible introducers

(11) Where the requirements of this paragraph are not met within a reasonable timeframe, the procedures must provide that –

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

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

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

Guidance on stopping and/or terminating business relationships/occasional transactions is at section 3.4.10.
Guidance on making internal disclosures is at section 5.4.

4.6 Insurance concessions

Code 20

Guidance on the insurance business specific concessions at paragraph 20 of the Code can be found in the Insurance Act 2008 sector specific guidance.

4.7 Miscellaneous concessions

Code 21

Paragraph 21 of the Code provides three miscellaneous concessions for retirement benefits for employees, collective investment schemes and the Isle of Man Post Office. Guidance on the first two concessions is below.

4.7.1 The concessions

4.7.1.1 Retirement benefits for employees

Code 21(1), 12(2)(b)

21 Miscellaneous

(1) 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).

It is for relevant persons to determine how to satisfy themselves that the retirement benefits scheme is as described and the conditions for use of the concession are met. All other AML/CFT/CPF requirements still apply. Further guidance can be found in the Private Pensions sector specific guidance.

4.7.1.2 Collective investment schemes

Code 21(2), 12(2)(b), Collective Investment Schemes Act 2008

21 Miscellaneous

(2) Where –

(a) a customer is –

(i) a collective investment scheme (except for a scheme within the meaning of Schedule 3 (exempt schemes) to the Collective Investment Schemes Act 2008), or

(ii) an equivalent arrangement in a jurisdiction in List C; and

(b) the manager or administrator of such a scheme or equivalent arrangement is -

(i) a regulated person; or

(ii) a person who acts in the course of external regulated business,

the relevant person need not comply with paragraph 12(2)(b).

Code 4(1), (2)

It is for relevant persons to determine the extent they need to go to, to ensure they are satisfied that the customer and its manager/administrator meet the requirements for this concession; on a case-by-case basis relative to the materiality and risk of ML/FT/PF. In making their determinations, relevant persons should bear in mind the principles and considerations set out in the CDD section of the Handbook on reliability of source documents data and information and the relevant person's risk assessments.

Relevant persons must ensure that the conditions for using the concession are met. In addition, all other AML/CFT/CPF requirements still apply.

4.7.2 Conditions on using the miscellaneous concessions

As with all the Code's concessions, they are subject to certain conditions.

4.7.2.1 ML/FT/PF risk assessment requirements

Code 21(4)(a), (1), (2), (3)

21 Miscellaneous

(4) Sub-paragraphs (1), (2) and (3) do not apply if –

(a) the customer is assessed as posing higher risk of ML/FT or;

Code 21(4), 6, 15

Assessing whether a customer poses a higher ML/FT/PF risk is done through the CRA and CRA reviews. Guidance on CRAs, including the higher risk factors specified in Code paragraph 15 is at section 2.2.9.

4.7.2.2 Identification of suspicious activity

Code 21(4)(b), (1), (2), (3)

21 Miscellaneous

(4) Sub-paragraphs (1), (2) and (3) do not apply if –

(b) the relevant person has identified any suspicious activity.

Code 21(5)

21 Miscellaneous

(5) If the relevant person has identified any suspicious activity the relevant person must make an internal disclosure.

Code 26, 27

These requirements should be read in the broadest sense in relation to the parties involved in the business relationship/occasional transaction. Guidance on suspicious activity and making internal and external disclosures is in chapter 5.

4.8 Transfer of a block of business

4.8.1 The concession

Code 22

To avoid unnecessary repetition and duplication of CDD processes and inconvenience to customers when business is transferred from one business to another, the Code allows the "purchaser" to rely on the CDD that has already been done on those customers by the "vendor". Acquisition of business or a block of business may be with or without consideration, either way, the concession at paragraph 22 may be used and the terms "purchaser" and "vendor" in this guidance are as per the Code.

Code 22(1), (2), (3)

22 Transfer of a block of business

(1) This paragraph applies where the relevant person (the **"purchaser"**) acquires a customer or group of customers from another relevant person (the **"vendor"**).

(2) The acquired customer or group of customers constitutes a new business relationship for the purchaser and customer due diligence in respect of that new business relationship may be provided to the purchaser by the vendor, if each of the conditions in sub-paragraph (3) are met.

Irrespective of whether an individual customer or a group of customers is acquired, all other AML/CFT/CPF requirements still apply, including risk assessment, ECDD, ongoing monitoring, sanctions screening and reporting requirements. The purchaser must ensure they are able to adhere to these requirements as well as the conditions for using this concession for each acquired customer at the outset of any acquisition and on a continuing basis.

4.8.2 Conditions for using the concession

4.8.2.1 Vendor status

Code 22(3)(a), (2), Collective Investment Schemes Act 2008, DBROA, Regulated Activities Order 2011

22 Transfer of a block of business

(3) The conditions referred to in sub-paragraph (2) are that –

(a) the vendor is, or was –

(i) a regulated person;

(ii) a collective investment scheme (except for a scheme within the meaning of Schedule 3 (exempt schemes) to the Collective investment Schemes Act 2008) where the manager or administrator of such a scheme is a regulated person, or where the vendor is an equivalent scheme in a jurisdiction in List C where the manager or administrator or that scheme is a person referred to in sub-head (iv);

(iii) a designated business; or

(iv) a person who acts in the course of external regulated business but does not solely carry on activities equivalent to either or both of Class 4 (corporate services) or Class 5 (trust services) under the Regulated Activities Order; and

The allowed vendor types listed are defined in the Code. Purchasing relevant persons must note that the concession cannot be used where the vendor is a non-Isle of Man corporate or trust service provider that would otherwise fall within the definition of external regulated businesses.

4.8.2.2 ML/FT/PF risk assessment requirements

Code 22(3)(b)(ii)

22 Transfer of a block of business

(3) The conditions referred to in sub-paragraph (2) are that –

(b) the purchaser -

(ii) undertakes a risk assessment of the customer and has not identified the customer as posing a higher risk of ML/FT;

Code 6(2)(a)

The concession only concerns CDD. As with any new business relationship /occasional transaction (by whatever means it is acquired), relevant persons must undertake a CRA on every customer to be acquired prior to the establishment of a business relationship/carrying out of an occasional transaction.

Code 6, 15

Assessing whether a customer poses a higher ML/FT/PF risk is done through the CRA and the CRA reviews. Guidance on CRAs is at section 2.2.9.

Where a customer is found to be higher risk (whether alone or within a block of customers), the concession must not be used in respect of that customer, though

it may still be used for other customers not assessed as higher risk within the same block.

It may not always be possible to undertake CRAs on every customer to be acquired before the acquisition takes place and the business relationships are established. In such cases, CRAs must be undertaken on every customer as soon as reasonably practicable. Where there is a delay in undertaking the CRAs, relevant persons are subject to unknown ML/FT/PF risks which they must manage and mitigate. Understanding the vendor's CRA procedures and risk classifications, may assist purchasing relevant persons to mitigate these potentially unknown ML/FT/PF risks for the limited duration it takes to perform its own CRAs. However, relevant persons must note that ML/FT/PF risk and the assessment of that risk is relative to each relevant person and business relationship/occasional transaction. Consequently, they cannot rely on the vendor's CRA.

4.8.2.3 Purchaser CDD requirements

22(3)(b)(i), (iii), (iv), (vi), (2)

22 Transfer of a block of business

(3) The conditions referred to in sub-paragraph (2) are that –

(b) the purchaser -

(i) has identified the customer and any beneficial owner of the customer and has no reason to doubt those identities;

…

(iii) knows the nature and intended purpose of the business relationship;

(iv) has taken reasonable measures to establish the source of funds;

…

(vi) has put in place appropriate measures to remedy, in a timely manner, any deficiencies in the customer due diligence of the acquired customer or group of customers.

Code 8(3)(a), 11(3)(a), 12

The requirements to identify the customer and any beneficial owner is in accordance with paragraphs 8(3)(a), 11(3)(a) and 12 of the Code. Guidance for which is at section 3.5.

Guidance on the nature and intended purpose of the business relationship or occasional transaction is at section 3.7.
Guidance on establishing source of funds is at section 3.8.

Initially, measures to remedy CDD deficiencies, could include reviewing the vendor's CDD procedures to determine whether there are any general concerns.

Measures to remedy CDD deficiencies should then include:

- reviewing the CDD for each customer acquired in conjunction with the CRA to determine whether there are any specific deficiencies to remedy in each case;
- determining whether it is necessary to collect additional CDD or make further enquiries either from the customer or from other sources; and
- taking steps to remedy the deficiencies.

4.8.2.4 Identification of suspicious activity

Code 22(3)(b)(v), (2)

22 Transfer of a block of business

(3) The conditions referred to in sub-paragraph (2) are that –

(b) the purchaser -

(v) has not identified any suspicious activities;

Code 26,27

Guidance on suspicious activity and making internal and external disclosures is in chapter 5.

4.8.2.5 ECDD requirements

Code 22(4), 15

22 Transfer of a block of business

(4) Where a customer has been identified by the vendor or purchaser as posing a higher risk of ML/FT the purchaser must undertake its own enhanced customer due diligence in respect of that customer in accordance with paragraph 15.

Purchasing relevant persons should adopt procedures to seek the risk classifications the vendor applied to the transferred customers. To ensure a comprehensive understanding of the vendor's applied risk classifications, the purchaser will also need to understand the vendor's CRA procedures including their risk classification parameters.

Code 6, 15

Guidance on CRAs is at section 2.2.9.
Guidance on ECDD where customers are assessed as higher risk as at section 3.4.7.

5. Reporting and registers

5.1 Introduction

Code Part 7

Part 7 of the Code sets out procedural requirements regarding the MLRO, reporting procedures and the disclosure of suspicious activity and sanctions breaches.

The competent authority in relation to the disclosure of suspicions is the IOMFIU The IOMFIU Guidance is the primary guidance on this subject. Its contents include:

- what is a Suspicious Activity Report[13] ("SAR");
- how a SAR must be submitted and what information must be included;
- submitting a quality SAR;
- what is suspicion;
- tipping off;
- consent to carry out specified activities; and
- disclosures under section 24 of the Financial Intelligence Unit Act 2016; and
- sanctions.

Also of note is that the FIU is currently working to establish "Public-Private Partnerships" ("PPPs"). A PPP is a collaboration between public and private sector entities working together as a partnership to achieve mutually beneficial outcomes. In the context of combatting financial crime, this takes the form of a partnership between the FIU, law enforcement, regulators and the financial sector to exchange and analyse information relating to ML/FT/PF and other wider

[13] Referred to in the Code as an external disclosure.

economic threats. If required, further information can be obtained from the FIU regarding PPPs by sending an email using this link.

The competent authority in relation to the administration of United Nations and UK financial and trade sanctions and export licensing controls in the Isle of Man is the ~~IOMCE~~IOMCI. The ~~IOMCE's~~IOMCI's website provides information and the Island's primary guidance on:

- financial sanctions;
- current sanctions regimes;
- terrorism and terrorist financing;
- proliferation and proliferation financing;
- export control and trade control; and
- trade based money laundering.

Reports in respect of both suspicious activity and financial sanctions are made to the IOMFIU via Themis, the IOMFIU's secure online reporting system. Details, and the Themis User Guide can be found on the IOMFIU's website.

5.1.1 Relevant legislation

Code 42

The Code contains obligations which relevant persons must meet in relation to the prevention and detection of ML/FT/~~FP.~~PF/. Paragraph 42 of the Code details the offences in relation to contravening the Code.

Offences in relation to ML/FT/~~FP~~PF/ (including offences in relation to failure to disclose) are contained in a number of other pieces of legislation:

- the POCA;
- the ATCA; and
- the TOCFRA.

All Isle of Man primary legislation can be found here and all Isle of Man secondary legislation can be found here.

5.2 Money Laundering Reporting Officers and Deputy Money Laundering Reporting Officers

Code 23, 25, 27

23 Money Laundering Reporting Officer

(1) A relevant person must appoint a Money Laundering Reporting Officer ("**MLRO**") to exercise the functions required under paragraphs 25 and 27.

(2) To be effective in the exercise of those functions an MLRO must –

(a) be sufficiently senior in the organisation of the relevant person or have sufficient experience and authority;

(b) have a right of direct access to the officers of the relevant person;

(c) have sufficient time and resources to properly discharge the responsibilities of the position; and

(d) retain responsibility for all external disclosures, including where a branch or subsidiary is in another jurisdiction.

A relevant person may appoint a Deputy Money Laundering Reporting Officer ("**Deputy MLRO**") in order to exercise the functions required under paragraphs 25 and 27 in the MLRO's absence.

Code 24, 23, IA 2008

24 Money Laundering Reporting Officer: insurers, insurance intermediaries and insurance managers

(1) Without limiting paragraph 23, the MLRO of an insurer, an insurance intermediary or an insurance manager must –

(a) in the case of an insurer authorised under section 8 of the Insurance Act 2008, an insurance intermediary or an insurance manager registered under section 25 of the Insurance Act 2008, be resident on the Island;

(b) be treated as a principal control officer for the purposes of the notice required under section 29(1) of the Insurance Act 2008; and

(c) be sufficiently senior in the organisation or have sufficient experience and authority including where the MLRO is not an employee of the insurer[14].

(2) Where an MLRO holds more than one appointment sub-paragraph (1) applies to each appointment.

If appointed, the Deputy MLRO should be of similar status and experience to the MLRO. Please note that licenceholders subject to the Financial Services Rule Book 2016 must appoint a Deputy MLRO as per Rule 8.21 (Head of compliance and MLRO). Where this Handbook refers to the MLRO this includes the Deputy MLRO in the MLRO's absence.

Code 4, 23, 24, 25, 26, 27

Relevant persons must ensure that the person they appoint as MLRO is able to fulfil their duties effectively, and as such should ensure that they are present and available to the staff of the relevant person to receive and review internal disclosures, make external disclosures and to liaise with the Isle of Man competent authorities. It should be noted that paragraph 24(1) of the Code requires that the MLRO of an insurer authorised under section 8 of the Insurance Act 2008, an insurance intermediary, or an insurance manager, to be resident in the island[15].

No further guidance is provided in respect of the other requirements of paragraphs 23 and 24.

[14] For example is part of an insurance manager.

[15] Please note that licenceholders subject to the Financial Services Rule Book 2016 must appoint a Head of compliance who is resident in the island, as per rule 8.21 (Head of compliance and MLRO).

5.3 Reporting procedures and requirements

Code 25, 28, 29

25 Reporting procedures

A relevant person must establish, record, maintain and operate reporting procedures and controls that –

(a) enable its officers and all other persons involved in its management, and all appropriate employees and workers to know to whom any suspicious activity is to be disclosed;

(b) ensure that there is a clear reporting chain to the MLRO;

(c) require an internal disclosure to be made to the MLRO if any information, or other matters that come to the attention of the person handling that business, are in that person's opinion suspicious activity;

(d) ensure that the MLRO has full access to any other information that may be of assistance and that is available to the relevant person;

(e) require the MLRO to consider internal disclosures in light of all other relevant information available to the MLRO for the purpose of determining whether the activity is, in the MLRO's opinion, suspicious activity;

(f) enable the information to be provided as soon as is practicable to the Financial Intelligence Unit as an external disclosure if the MLRO knows or suspects, or has reasonable grounds for knowing or suspecting, that the activity is ML/FT and;

ensure the registers required by paragraphs 28 and 29 are maintained and completed in accordance with those paragraphs.

Code 26, 15

26 Internal disclosures

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, unless the relevant person reasonably believes conducting enhanced customer due diligence will tip off the customer; and

(b) make an internal disclosure.

Code 27, 25

27 External disclosures

(1) Where an internal disclosure has been made, the MLRO must assess the information contained within the disclosure to determine whether there are reasonable grounds for knowing or suspecting that the activity is ML/FT.

(2) The MLRO must make an external disclosure to the Financial Intelligence Unit in accordance with the reporting procedures and controls established under paragraph 25 as soon as is practicable if the MLRO –

(a) knows or suspects; or

(b) has reasonable grounds for knowing or suspecting,

that the activity is ML/FT.

(3) A disclosure under sub-paragraph (2) does not breach –

(a) any obligation of confidence owed by the MLRO; or

any other restrictions on the disclosure of information (however imposed).

5.3.1 Suspicious activity

Making internal and external disclosures[16] necessitates identifying activity which is suspicious, as opposed to activity which is unusual.

Code 3(1)

3 Interpretation

(1) In this Code –

"suspicious activity" means any activity, including the receipt of information, which in the course of a business relationship, occasional transaction or attempted transaction causes the relevant person to –

(a) know or suspect; or

(b) have reasonable grounds for knowing or suspecting,

that the activity is ML/FT or that the information is related to ML/FT;

Code 27(1) , (2)

Relevant persons and MLROs need to be able to demonstrate their compliance with AML/CFT/CPF requirements. Fully documenting the reasons for decisions can assist with this.

Guidance regarding suspicion can be found in the IOMFIU Guidance for making SARs and the FIU Guidance Note regarding "suspicion" as per POCA and ATCA.

Code 13(3), 26

Where a relevant person identifies suspicious activity they must comply with the requirements of paragraphs 13(3) and 26.

Guidance on ongoing monitoring can be found in section 3.4.6.
Guidance on ECDD can be found in section 3.4.7.
Guidance on internal disclosures can be found in section 5.4.

5.4 Disclosures

Code 25 , 28, 29

25 Reporting procedures

[16] If you as the MLRO identify suspicious activity, an internal disclosure can be considered as being made when preparing or recording the information prior to externalising this to the FIU through Themis. For guidance regarding how to record this in the annual AML/CFT statistical return please refer to the Strix guidance document.

A relevant person must establish, record, maintain and operate reporting procedures and controls that –

(a) enable its officers and all other persons involved in its management, and all appropriate employees and workers to know to whom any suspicious activity is to be disclosed;

(b) ensure that there is a clear reporting chain to the MLRO;

(c) require an internal disclosure to be made to the MLRO if any information, or other matters that come to the attention of the person handling that business, are in that person's opinion suspicious activity;

(d) ensure that the MLRO has full access to any other information that may be of assistance and that is available to the relevant person;

(e) require the MLRO to consider internal disclosures in light of all other relevant information available to the MLRO for the purpose of determining whether the activity is, in the MLRO's opinion, suspicious activity;

(f) enable the information to be provided as soon as is practicable to the Financial Intelligence Unit as an external disclosure if the MLRO knows or suspects, or has reasonable grounds for knowing or suspecting, that the activity is ML/FT and;

(g) ensure the registers required by paragraphs 28 and 29 are maintained and completed in accordance with those paragraphs.

Relevant persons must ensure that all employees are made aware of the identity of the MLRO (and the Deputy MLRO if there is one), and the procedure to follow when making an internal disclosure to the MLRO. Reporting lines should be as short as possible with a minimum number of people between the employee with suspicion and the MLRO. All internal disclosures must reach the MLRO without any undue delay. Under no circumstances should reports be intercepted by supervisors or managers such that they do not reach the MLRO.

All suspicions reported to the MLRO should be documented (in urgent cases this may follow an initial disclosure by telephone). The report should include the full details of the customer and as full a statement as possible of the information giving rise to the suspicion.

The MLRO should acknowledge receipt of the internal disclosure and, at the same time, remind the reporter of the provisions of POCA with regard to prejudicing investigations, and tipping off offences.

Code 27 (2)

Where an internal disclosure has been assessed by the MLRO and the MLRO has reasonable grounds for knowing or suspecting that the activity is ML/FT/PF an external disclosure must be made to the IOMFIU via Themis, as per paragraph 27 of the Code.

Code 27, 25

27 External disclosures

(1) Where an internal disclosure has been made, the MLRO must assess the information contained within the disclosure to determine whether there are reasonable grounds for knowing or suspecting that the activity is ML/FT.

(2) The MLRO must make an external disclosure to the Financial Intelligence Unit in accordance with the reporting procedures and controls established under paragraph 25 as soon as is practicable if the MLRO –

(a) knows or suspects; or

(b) has reasonable grounds for knowing or suspecting,

that the activity is ML/FT.

(3) A disclosure under sub-paragraph (2) does not breach –

(a) any obligation of confidence owed by the MLRO; or

(b) any other restrictions on the disclosure of information (however imposed).

Further information on external reporting is in the IOMFIU guidance.

5.5 Registers of disclosures

Code 28

28 Registers of disclosures

(1) A relevant person must establish and maintain separate registers of –

(a) all internal disclosures;

(b) all external disclosures; and

(c) any other disclosures to the Financial Intelligence Unit.

(2) The registers must include details of –

(a) the date on which the disclosure is made;

(b) the person who made the disclosure;

(c) for internal disclosures, whether it is made to the MLRO or the deputy MLRO;

(d) for external disclosures, the reference number supplied by the Financial Intelligence Unit; and

The registers of disclosures required by sub-paragraph (1) may be contained in a single document if the details required to be included in those registers under sub-paragraph (2) can be presented separately for each type of disclosure on request by a competent authority.

Paragraph 28 details the requirements in relation to registers of disclosures. No further guidance is provided.

5.6 Register of money laundering and financing of terrorism enquiries

Code 29

29 Register of money laundering and financing of terrorism enquiries

(1) A relevant person must establish and maintain a register of all ML/FT enquiries received by it from competent authorities.

(2) The register must be kept separate from other records and include –

(a) the date of the enquiry;

(b) the nature of the enquiry;

(c) the name and agency of the enquiring officer;

(d) the powers being exercised; and

(e) details of the account or transactions involved.

Relevant persons may receive enquiries from competent authorities regarding ML/FT/PF. As per paragraph 29 of the Code, relevant persons must establish and maintain a register of all enquiries received by them from competent authorities.

FIUA

If a relevant person receives a request under section 18 (Power to gather additional information) of the Financial Intelligence Unit Act 2016 ("FIUA"), this must be recorded on the register of ML/FT/PF enquires, but in the event the Authority requests to review the register as part of any supervisory work, references to requests under section 18 of the FIUA must be redacted, unless the consent of the IOMFIU is obtained to disclose the information to the Authority as per sections 25 and 26 (Restrictions on further disclosure and Offence for failing to comply with restriction on further disclosure) of the FIUA.

5.7 Suspicious activity reporting of declined business

FIUA

If a relevant person declines to take on business because they know or suspect that the business involves ML/FT/PF they must submit a SAR to the IOMFIU. If business is declined for other reasons which the relevant person thinks may be of interest to the IOMFIU, a disclosure can be made under section 24 of the FIUA. Information which is not specifically to do with ML/FT/PF but may relate to other criminality helps the IOMFIU and law enforcement authorities to understand the ML/FT/PF threat to the Island.

5.8 Data protection law

Code 27(3)(b)
POCA 153

Data protection legislation makes specific exemptions for disclosures authorised under other law; section 153 of POCA creates a specific authorisation to disclose (despite any restriction on the disclosure of information (however imposed)) provided that certain conditions are met:

153 Protected disclosures

(1) A disclosure which satisfies the following three conditions is not to be taken to breach any restriction on the disclosure of information (however imposed).

(2) The first condition is that the information or other matter disclosed came to the person making the disclosure (the discloser) in the course of the discloser's trade, profession, business or employment.
(3) The second condition is that the information or other matter –
(a) causes the discloser to know or suspect; or
(b) gives the disclosure reasonable grounds for knowing or suspecting,
that another person is engaged in money laundering.
(4) The third condition is that the disclosure is made to –
(a) the FIU; or
(b) a nominated officer
as soon as is practicable after the information or other matter comes to the discloser.

Further information about data protection can be found on the Information Commissioner's website.

5.9 Handling of suspicion in outsourced back office functions

Code 4(3)

Where a relevant person is undertaking AML/CFT/CPF work for other entities, it is important that both entities are aware of their obligations under the Code. All entities which are relevant persons must comply with all requirements of the Code. Whilst work may be delegated or outsourced, the ultimate responsibility for compliance with the Code is always that of the regulated person.

In cases where one relevant person (person A) is providing services to another relevant person (person B) and person A detects suspicious activity in relation to person B's customers it is acceptable for one external report to be submitted on behalf of both person A and person B. Where this is done the external disclosure should clearly state in the grounds section that it is being made on behalf of both person A and person B.

Where a relevant person is conducting work for an entity in another jurisdiction (a 'foreign entity') the foreign entity must be in compliance with the AML/CFT/CPF regime it is subject to. The relevant person must comply with the Code.

If the relevant person is providing the MLRO for the foreign entity and makes a disclosure to the financial intelligence unit or law enforcement agency of that jurisdiction a disclosure must also be made to the IOMFIU. This is known as dual reporting; further information regarding this can be found in the IOMFIU's guidance.

6. Compliance and record keeping

6.1 Monitoring and testing compliance

Code 30(1), 5

30 Monitoring and testing compliance

(1) A relevant person must establish, record, maintain and operate appropriate procedures and controls for monitoring and testing compliance with the AML/CFT legislation, so as to ensure that -

(a) the relevant person has robust and recorded arrangements for managing the risks identified by the business risk assessment carried out in accordance with paragraph 5;

(b) the operational performance of those arrangements is suitably monitored; and

(c) prompt action is taken to remedy any deficiencies in arrangements.

Code 4(2), 30

Paragraph 30 of the Code refers to the monitoring and testing by relevant persons to ensure that their processes and procedures (and the operation of these processes and procedures) comply with the AML/CFT/CPF legislation, and that relevant persons are sufficiently managing and mitigating the risks of ML/FT/PF identified by their BRA.

Code 4(1)(a)

The procedures and controls referred to in paragraph 30(1) of the Code must enable relevant persons to manage and mitigate their ML/FT/PF risks and assist in ensuring their compliance with AML/CFT/CPF legislation. Monitoring and testing should be undertaken commensurate with the nature and scale of the relevant person. The monitoring and testing compliance procedures established must be appropriate for the purposes of forestalling and preventing ML/FT/PF.

Code 4(2)(c)

Such procedures must be approved by the senior management of the relevant person.

Code 30(2), (1)

30 Monitoring and testing compliance

(2) A report to the senior management of the relevant person must be submitted, at least annually, describing –

(a) the relevant person's AML/CFT environment including any developments in relation to AML/CFT legislation during the period covered by the report;

(b) progress on any internal developments during the period covered by the report in relation to the relevant person's policies and procedures and controls for AML/CFT;

(c) any activities relating to compliance with this Code that have been undertaken by the relevant person during the period covered by the report; and

(d) the results of any testing undertaken in accordance with sub-paragraph (1).

Code 4(2)(b)

The report should enable senior management to not only be aware of the ML/FT/PF risks to which the relevant person is exposed but also to understand how effective the relevant person's AML/CFT/CPF framework is in mitigating these risks. Relevant persons must determine the level of detail to be contained in this report, making sure that it is specific to them and the nature, scale and complexity of their business.

For further information see the Supplemental Information Document which includes a non-exhaustive, non-limited list of examples of what could be included.

Code 30 (3), (4)

30 Monitoring and testing compliance

(3) A relevant person must ensure that there is a suitable person at management level that is responsible for the functions specified in this paragraph.

(4) To be effective in the exercise of the functions the suitable person must –

(a) be sufficiently senior in the organisation of the relevant person or have sufficient experience and authority;

(b) have a right of direct access to the officers of the relevant person; and

(c) have sufficient time and resources to properly discharge the responsibilities of the position.

Generally, the Authority's expectation in relation to regulated firms[17] is that the suitable person with responsibility for the requirements of Section 30 of the Code would be the Head of Compliance of the firm (Controlled function R13). In relation to registered[18] firms we would expect this to be the compliance officer (where appointed). The Authority notes that smaller registered firms may not have a dedicated compliance or AML/CFT/CPF resource to be this suitable person, in such cases it is useful to be pragmatic while trying to ensure the monitoring/testing is

[17] Either licensed under the Financial Services Act 2008 or the Insurance Act 2008.
[18] Registered under the Designated Businesses (Registration and Oversight) Act 2015.

independent from the person who designed the procedures or undertook the task, though it is recognised this may not always be possible.

6.2 New staff appointments

Code 31

31 New staff appointments

A relevant person must establish, record, maintain and operate appropriate procedures and controls to enable the relevant person to satisfy itself of the integrity of new officers of the relevant person and of all new appropriate employees and workers.

The procedures and controls must have regard to the materiality and risk of ML/FT/PF and enable the relevant person to manage and mitigate these risks.

Relevant persons must determine which staff fall into the category of appropriate employees and workers based on the nature and scope of their role and having regard to the risk of ML/FT/PF[19]. These requirements are not limited to high level staff such as MLROs, Deputy MLROs, Heads of Compliance and Compliance Officers (where appointed), they may also include other members of staff such as customer facing staff where there are ML/FT/PF risks or members of the compliance department.

The type and extent of procedures and controls undertaken should be proportionate to the ML/FT/PF risks associated with the particular role within the organisation and the particular employee/worker employed to fulfil that role.

Examples of ways for relevant persons to satisfy themselves of the integrity of new staff include, but are not limited to:

- obtaining and confirming references;
- confirming employment history and the qualifications advised;
- requesting details of any regulatory action taken against the individual (or confirmation that no regulatory action has been taken);
- conducting open source checks; and
- requesting details of any criminal convictions (or confirmation that there are no criminal convictions) and verify where possible.

Relevant persons should document the steps taken to satisfy the requirements of the Code, including any information and confirmations obtained. Relevant persons should also document where they have decided not to, or it has not been possible to, obtain the information they would generally request, including the reasons why this is the case.

[19] Where appropriate, relevant persons should be aware of the Fitness and Propriety guidance applicable to their sector which must be complied with.

6.3 Staff training

Code 4(2)

Effective application of AML/CFT/CPF policies and procedures depends on the relevant persons' staff understanding the relevant requirements and accompanying processes and procedures they are required to follow as well as the risks that the processes and procedures are designed to mitigate (including sufficient training regarding any technology used, as discussed in section 2.2.11.2~~)~~ ~~.~~). Training carried out by relevant persons should be designed to mitigate potential AML/CFT/CPF risks occurring by, at or through the relevant person as well as ensuring that staff have an understanding of the AML/CFT/CPF environment.

Code 32

32 Staff training

(1) A relevant person must provide or arrange education and training, including refresher training, at least annually, for:

(a) all officers;

(b) any other persons involved in its senior management; and

(c) appropriate employees and workers.

Relevant persons must ensure that the education and training provided is undertaken periodically, and at any rate at least annually. This is to ensure employees are kept up-to-date and aware of AML/CFT/CPF developments in order that the relevant person is able to manage and mitigate their ML/FT/PF risks.

Code 3(1), 32(1),(b), (c)

The Code includes definitions of "employee" and "worker". Relevant persons should consider the risks posed by different roles to determine who are appropriate employees and workers for the purposes of paragraph 32(1)(c) of the Code. Relevant persons should also consider that a member of staff may require training as a result of being part of senior management, as per 32(1)(b), regardless of their specific day to day role.

Code 32(1), (2)

Training must be risk sensitive and relevant to a person's role; therefore, different training may be required for different roles. The training for each category of persons listed in paragraph 32(1) should include all the elements listed in paragraph 32(2), though the extent and detail of such training may be tailored according to the particular employee's role within the relevant person. Consequently, the MLRO and Deputy MLRO (if appointed) should receive more detailed training commensurate with the requirements, responsibilities and AML/CFT/CPF risks of their roles.

Code 4(2)

Relevant persons must be mindful of the overarching requirement to ensure their procedures and controls are risk sensitive and enable them to manage and mitigate their ML/FT/PF risks. Consequently, though not explicitly stated in the Code, relevant persons should also ensure that employees and staff have an appropriate level of knowledge regarding the relevant person's products and

services, what their 'normal use' is and how they may be abused for the purposes of ML/FT/PF.

Where a relevant person uses technology as part of their procedures and controls in relation to AML/CFT/CPF they should ensure that staff are provided with appropriate training regarding this technology, including its benefits and limitations.

Code 32(3), (1)

32 Staff training

(3) Where there have been significant changes to AML/CFT legislation, or the relevant person's policies and procedures, the relevant person must provide appropriate education and training to the persons referred to in sub-paragraph (1) within a reasonable timeframe.

Code 32(1)

If it is deemed that changes have taken place which require particular training, this training must be in addition to the regular training delivered under paragraph 32(1).

Relevant persons must determine whether changes to legislation, policies or procedures require specific education and training, taking into account the materiality and risk of ML/FT/PF.

Code 32(4)

32 Staff training

(4) The relevant person must maintain records which demonstrate compliance with this paragraph.

Code 32

Maintaining training records enables relevant persons to demonstrate that they have complied with the requirements of paragraph 32 of the Code and have equipped their staff with appropriate knowledge.

6.4 Record keeping, retention, format and retrieval

Code 33

Record keeping is an essential part of meeting the Code requirements to ensure criminal and terrorist property can be traced and confiscated and persons involved can be investigated and prosecuted.

Code 4

Record keeping procedures and controls must be sensitive to ML/FT/PF risk and enable the relevant person to manage and mitigate their ML/FT/PF risks. Furthermore, satisfactory record keeping is paramount for relevant persons themselves in ensuring they are able to comply with their obligations under the AML/CFT/CPF legislation. A relevant person's record keeping procedures and controls must enable them to satisfy, within a reasonable time frame, any enquiries from competent authorities.

Furthermore, it is only through adequate record keeping that relevant persons can demonstrate compliance with AML/CFT/CPF legislation; for example, to the relevant person's auditors, supervisors or in the event of legal enquiries.

6.4.1 Records concerning risk assessments, due diligence and monitoring, branches and subsidiaries and correspondent services

Code 33(a), 37, 38, 38, Parts 3, 4, 5, 6

33 Record keeping

A relevant person must keep –

> (a) a copy of the documents obtained or produced under Parts 3 to 6, paragraphs 37 and 39, including identification information, account files, business correspondence records and the results of any analysis undertaken (or information that enables a copy of such documents to be obtained);

Code 33(a)

Whilst paragraph 33(a) lists some specific types of documentation which must be kept by relevant persons this is not exhaustive. The record keeping requirements are wider than just CDD documents. Relevant persons must keep copies of all documents maintained or produced under the parts and paragraphs listed in paragraph 33(a).

Records relating to verification of identity should comprise the evidence itself or a copy of it or, if that is not readily available, information reasonably sufficient to obtain such a copy should be included.

Code 4(2), (3), 17, 19

It may be possible to rely on third parties for certain aspects of CDD (when utilising paragraph 17 or paragraph 19), or outsourcing certain practical CDD steps to others, it is not possible to outsource responsibility for compliance with any of the Code's requirements. The Authority would expect that where any reliance on third parties is used within the CDD process the relevant person will ensure that the third parties are aware of the record keeping requirements of the Code and that this is covered in any terms of business or agreements where applicable.

6.4.2 Transaction records

Code 33(b), (c)

> **33 Record keeping**
>
> A relevant person must keep –
>
> (b) a record of all transactions carried out in the course of business in the regulated sector, including identification information, account files, business correspondence records and the results of any analysis undertaken (or information that enables a copy of such records to be obtained); and
>
> (c) such other records as are sufficient to permit reconstruction of individual transactions and compliance with this Code.

Relevant persons must ensure that that records they keep are appropriate for the purposes of forestalling and preventing ML/FT/PF and enable them to manage and mitigate the risks of ML/FT/PF that they have identified. In relation to records of transactions, relevant persons must keep records which ensure that:

- any transactions or instructions effected via the relevant person on behalf of any individual customer can be reconstructed; and
- the audit trail for funds entering and leaving the relevant person is clear and complete.

In order to permit the reconstruction of transactions, some of the following may be relevant:

- details of the customer (or other parties to the transaction), including account details;
- the nature and details of the transaction;
- the volume of funds flowing through the account/turnover of client entity;
- the origin of the funds;
- the form in which the funds were offered or withdrawn, i.e. cash, cheque etc.;
- the identity of the person undertaking the transaction;
- the destination of the funds;
- the form of instruction and authority;
- the name and address (or identification code) of the counter party the security dealt in, including price and size (if applicable);
- whether the transaction was a purchase or a sale;
- the account details from which the funds were paid (including, in the case of cheques, bank name, sort code, account number, IBAN number and name of account holder);
- the form and destination of payment made by the business to the customer;
- whether the investments were held in safe custody by the business or sent to the customer or to their order and, if so, to what name and address;
- activities of the client entity; and
- any large item/exception reports created in the course of transaction monitoring.

6.4.3 Record retention

Code 34

34 Record retention

(1) A relevant person must keep the records required by this Code for at least the period specified in sub-paragraph (3) or (4).

(2) To avoid doubt, the obligation in sub-paragraph (1) continues to apply after a person ceases to be a relevant person.

Code 34(2)

Businesses to which paragraph 34(2) of the Code applies include businesses who have been struck off, dissolved or who have re-domiciled and have been discontinued.

No further guidance is provided in relation to the other requirements of paragraph 34.

6.4.4 Electronically stored records

Code 35(2)(c)

35 Record format and retrieval

(2) In the case of any records required to be established and maintained under this Code –

(c) if the records are not in the form of hard copies (such as records kept on a computer system), the relevant person must ensure that they are readily accessible in or from the Island and that they are capable of retrieval without undue delay.

Code 5, 7, 35

Where a relevant person chooses to implement an electronic storage system, an assessment of the risks must be undertaken in line with paragraph 7 of the Code and this should be factored into the BRAs and TRAs undertaken under paragraphs 5 and 7 of the Code. It is up to the relevant person whether they determine it appropriate to retain the originals of documents which are stored electronically.

7. Miscellaneous

7.1 Branches, subsidiaries and agents

Code 274(1), (7), POCA s 4

37 Branches, subsidiaries and agents

This paragraph applies to a relevant person if a branch or subsidiary is undertaking an activity which is equivalent to any activity included in Schedule 4 to the Proceeds of Crime Act 2008.

37 Branches, subsidiaries and agents

In this paragraph, a "branch or subsidiary" mean a branch or majority owned subsidiary of the relevant person in a jurisdiction outside the island.

A relevant person in the Isle of Man may have overseas branches, subsidiaries or agents. In such cases, control must be exercised over business equivalent to any activity included in Schedule 4 to POCA which is conducted outside of the Isle of Man. Alternatively, elements of the Isle of Man regulated business may have been outsourced to other jurisdictions.

Code 37(2)

37 Branches, subsidiaries and agents

(2) A relevant person must ensure that a branch or subsidiary takes measures consistent with this Code and guidance issued by a competent authority for AML/CFT.

This does not mean that the measures must mirror those of the Isle of Man in every detail, rather, that the measures should be of an equivalent or consistent standard to those in the Isle of Man. In such cases, a relevant person may consider establishing a group AML/CFT/CPF strategy to protect its global reputation as well as its Isle of Man business.

The branch, subsidiary or agent is subject to the AML/CFT/CPF regime of the jurisdiction that it is established in, and must ensure that it complies with this, including the reporting requirements of that jurisdiction.

Code 37 (3), (2), (4), (5)

37 Branches, subsidiaries and agents

(3) A relevant person who cannot comply with sub-paragraph (2) for any reason must apply appropriate additional measures to manage the ML/FT risk.

(4) Without limiting sub-paragraph (3), a reason for being unable to comply with sub-paragraph (2) may include being prevented from doing so by the laws or regulations of the jurisdiction to which the branch or subsidiary is subject.

(5) A relevant person must inform the relevant competent authority immediately when the person or a branch or subsidiary is unable to take any of the measures referred to in sub-paragraph (2).

Code 4(3), 372), (5)

Additionally, where a host county prevents compliance that is at least in line with the Code relevant persons must apply appropriate additional measures to manage ML/FT/PF risks and inform the Authority of the measures that are being taken.

Code 37(6), 4, Regulated Activities Order 2011

37 Branches, subsidiaries and agents

(6) If a relevant person is licensed under Class 8(2)(a) (provision and execution of payment services directly) of the Regulated Activities Order the relevant person must ensure that any agents they use or operate through, are included in the relevant person's procedures and controls required by paragraph 4. The relevant person must also monitor compliance of the agent with the requirements.

No guidance is provided in relation to paragraph 37(6).

7.2 Shell banks

Code 3(1)

3 Interpretation

(1) In this Code -

"shell bank" means a bank (or shell securities provider) that is –

(a) incorporated in a jurisdiction in which it has no physical presence; and

(b) not affiliated with a financial services group that is subject to effective consolidated supervision,

Code 38(1), (2)

38 Shell banks

(1) A relevant person must not –

(a) enter into or continue a business relationship; or

(b) carry out an occasional transaction,

with a shell bank.

(2) A relevant person must take adequate measures to ensure that –

(a) it does not enter into or continue a business relationship; or

(b) carry out an occasional transaction,

with a respondent institution that permits its accounts to be used by a shell bank.

Jurisdictions are unlikely to be able to exercise adequate supervision over a shell bank's compliance with AML/CFT/CPF requirements. In addition, within some jurisdictions, the licensing requirements for shell banks have historically been weak, permitting some shell banks to be operated by, or controlled by, individuals who are not fit and proper to do so.

Code 38

Relevant persons must establish, record, operate and maintain risk based procedures and controls for ensuring that they comply with the requirements of paragraph 38. The considerations regarding shell banks should be part of a relevant person's risk assessment, CDD and ongoing monitoring procedures and controls.

Guidance regarding risk assessments can be found in chapter 2.
Guidance regarding CDD can be found in chapter 1.
Guidance regarding ongoing monitoring can be found in section 3.4.6.

7.3 Correspondent services

Code 39

39 Correspondent services

(1) This paragraph applies to a business relationship or an occasional transaction, which involves correspondent services or similar arrangements.

(2) A relevant person must not enter into or continue a business relationship or carry out an occasional transaction to which this paragraph applies with a respondent institution in another jurisdiction unless it is satisfied that the respondent institution does not permit its accounts to be used by shell banks.

(3) Before entering into a business relationship or carrying out an occasional transaction to which this paragraph applies, a relevant person must –

(a) obtain and document sufficient information about the respondent institution to fully understand and risk assess the nature of its business and its customer base;

(b) determine from ~~publically~~publicly available information –

(i) the reputation of the respondent institution;

(ii) the quality of the supervision to which it is subject;

(iii) whether it has been subject to investigation or regulatory action in respect of ML/FT; and

(iv) whether the respondent institution is included on the sanctions list.

(c) assess and document the AML/CFT procedures and controls maintained by the respondent institution, and ascertain that they are adequate and effective;

(d) ensure that the approval of the relevant person's senior management is obtained; and

(e) clearly understand and document the respective responsibilities of each institution including the relevant person and the respondent institution with respect to AML/CFT measures.

(4) If a business relationship or occasional transaction to which this paragraph applies involves a payable-through account, a relevant person must be satisfied that the respondent institution –

(a) has taken measures that comply with the requirements of the FATF Recommendations 10 (Customer due diligence) and 11 (Record keeping) with respect to every customer having direct access to the account, and

(b) will provide on request the relevant person with relevant verification of the identity of the customer in accordance with this Code or to AML/CFT requirements at least equivalent to those in this Code.

(5) In the paragraph –

"**correspondent services**" means banking, money or value transfer services or other similar relationships provided by a financial institution or designated business in another jurisdiction ("**the respondent institution**"); and

"**payable-through account**" means an account maintained by a correspondent institution that may be operated directly by the customer of the respondent institution.

Code 4(2), 38, 39

When undertaking the requirements of paragraph 39 of the Code relevant persons should be aware that screening transactions though respondent institutions can be challenging due to the use of layered corporate entities and shell companies. However, not all correspondent relationships post the same level of ML/FT/~~FP~~PF risk and relevant persons must take a risk based approach to undertaking due diligence on correspondent relationships.

7.4 Fictitious, anonymous and numbered accounts

Guidance on fictitious, anonymous and numbered accounts is at section 3.3.2.