ISLE OF MAN
FINANCIAL SERVICES AUTHORITY

Lught-Reill Shirveishyn Argidoil Ellan Vannin

Authorised Insurers (Non-Life), Registered Insurance Managers, and Registered Insurance Intermediaries (General Business)

Sector Specific AML/CFT Guidance Notes

March 2022

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

Tel: 01624 646000
Email: aml@iomfsa.im
Website: www.iomfsa.im

Version 3
(First issued October 2019)

Contents

Version history

Version 2 (March 2020)	Updates made to links in relation to the updated NRA
Version 3 (March 2022)	Updates to reflect changes to the main structure of the AML/CFT Handbook Updates to footnotes to include links in the main body for consistency purposes 3 – further information added about who the customer is 3.2 – information added about delegation 3.4 – section added about the role of the Money Laundering Reporting Officer 3.5 – section added about external disclosures 4 – information added about risk assessments 5 – information added about risk assessment requirements 6 – section changed to 'Kidnap, ransom and cyber insurance'

1. Foreword

For the purposes of this sector specific guidance, "non-life" refers to the following:

- Authorised Insurers (businesses authorised under paragraph 8 of the Insurance Act 2008);
- Registered Insurance Managers (businesses registered under paragraph 25 of the Insurance Act 2008); and
- Registered Insurance Intermediaries (General Business) (businesses registered under paragraph 25 of the Insurance Act 2008).

Interpretation of these terms can be found in paragraph 54 of the Insurance Act 2008.

All legislation can be found at the Isle of Man Government's legislation website.

2. Introduction

The purpose of this document is to provide some guidance specifically for the non-life insurance sector in relation to anti-money laundering and countering the financing of terrorism ("AML/CFT"). This document should be read in conjunction both with the Anti-Money Laundering and Countering the Financing of Terrorism Code 2019 ("the Code") and the main body of the AML/CFT Handbook ("the Handbook").

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

This document covers unique money laundering and financing of terrorism ("ML/FT") risks that may be faced by the sector and provides further guidance in respect of approaches to customer due diligence where it may vary across between sectors.

The Authority recommends that relevant persons familiarise themselves with these documents and other typology reports concerning the non-life insurance sector. Also, some case studies are included to provide context to the risks of the sector.

2.1. National Risk Assessment

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

In relation to the main vulnerability of the sector, there is a risk that corporate structures may be established in order to channel funds to disguise their original source. The NRA sets out the main risks and vulnerabilities in detail.

Overall, after applying consideration of the control and other preventative measures in place and nature of the sector the non-life sector is assessed as having a medium low level of vulnerability for ML and TF.

3. Who is your customer?

Each relevant person must comply with the requirements of Part 3 of the Code and undertake business and technology risk assessments of their own business as well as customer risk assessments for each of their customers.

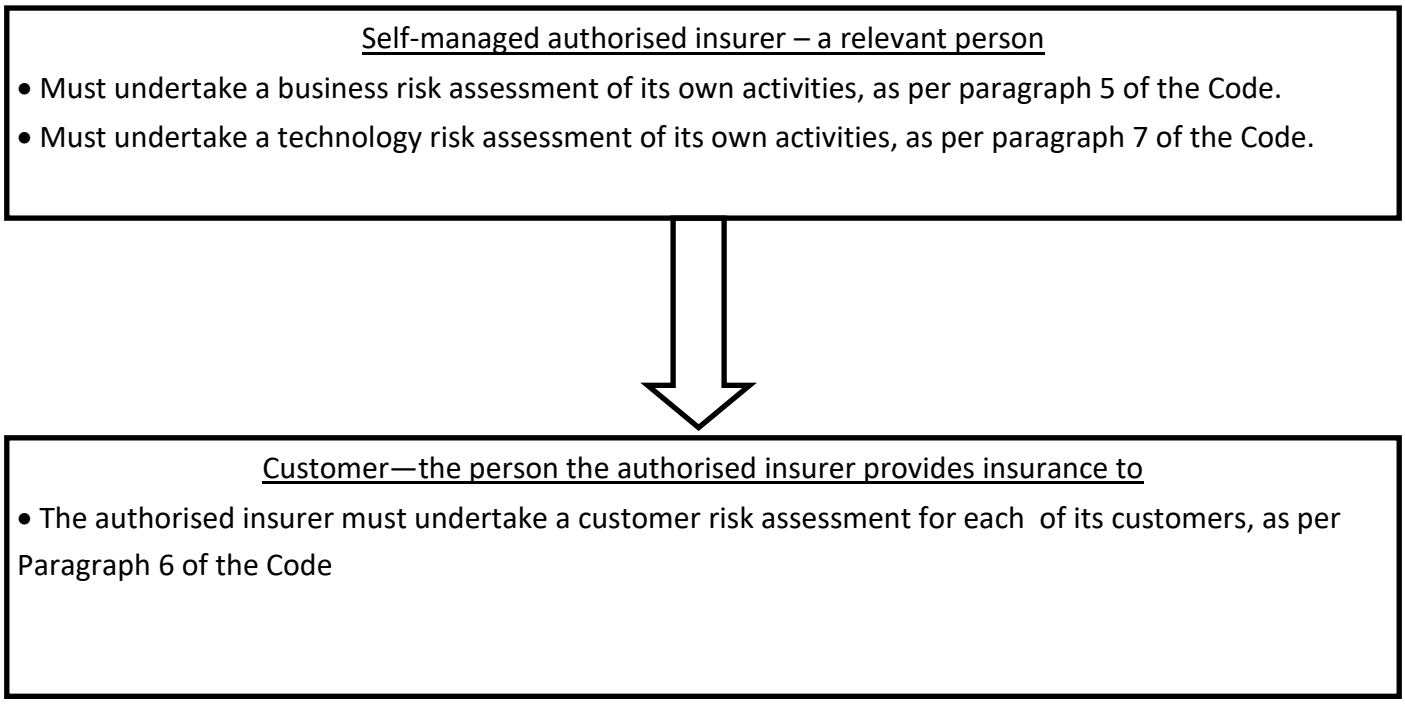
Broadly, a relevant person's customer is who they are contracting with[1] (which in relation to insurance companies will include policy holders), considering the definitions of "customer" and "business relationship" included in paragraph 3 of the Code. Relevant persons must also consider the requirements of paragraph 12(2)(b) of the Code and determine whether their customer is acting on behalf of another person, and if so identify that other person and take reasonable measures to verify that other person's identity using reliable, independent source documents, data or information. Further guidance regarding identifying who is the customer for different types of business can be found below.

As per paragraph 6 of the Code, customer risk assessments must be carried out for every customer. Guidance in relation to conducting risk assessments is provided in chapter 3 of the Handbook.

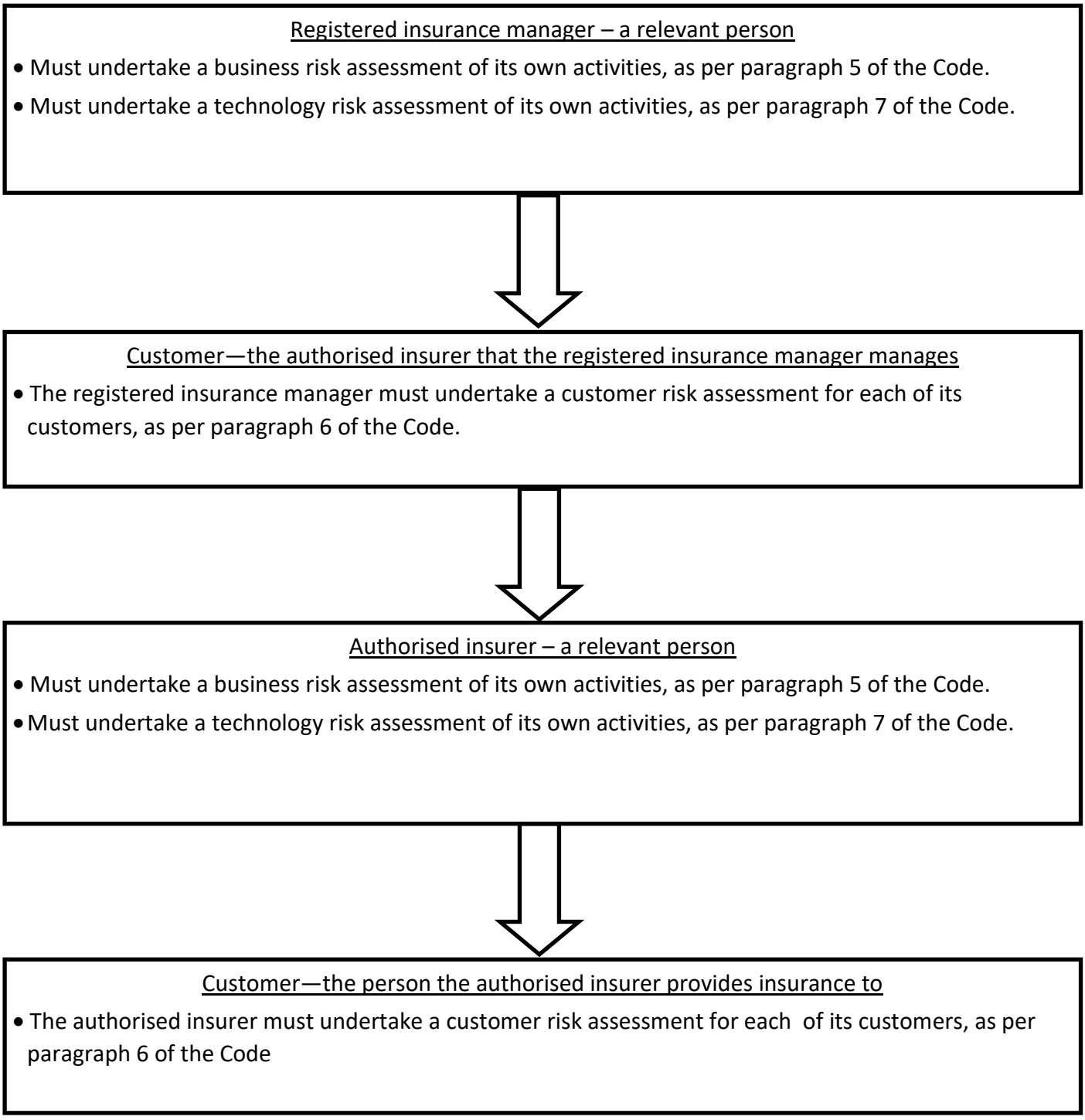
The diagrams below may assist in assessing who is your customer in this sector.

[1] As discussed in section 5 of this document, there may be a need to look through arrangements to consider the specific activity being insured.

3.1 Diagram 1

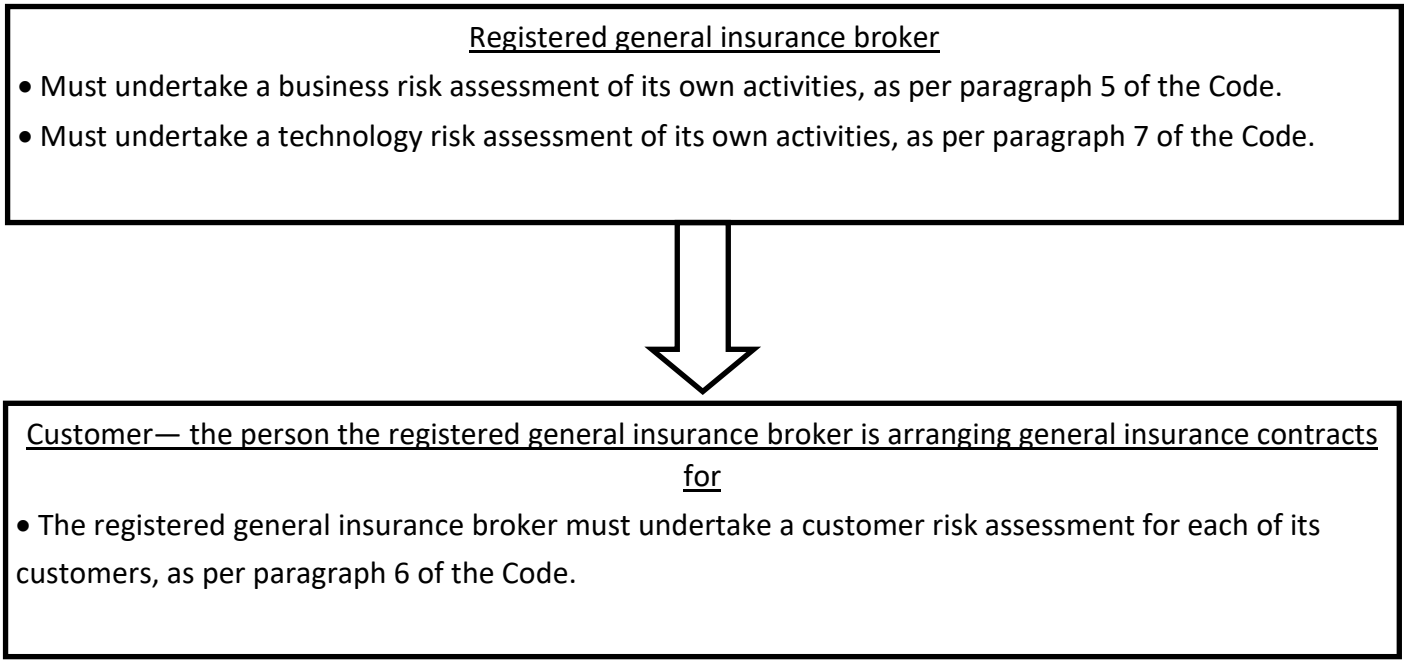

Self-managed authorised insurer – a relevant person
• Must undertake a business risk assessment of its own activities, as per paragraph 5 of the Code.
• Must undertake a technology risk assessment of its own activities, as per paragraph 7 of the Code.
Customer—the person the authorised insurer provides insurance to
• The authorised insurer must undertake a customer risk assessment for each of its customers, as per Paragraph 6 of the Code

3.2 Diagram 2



In practice a managed authorised insurer will delegate the majority (if not all) of AML/CFT activities to its registered insurance manager; however, the authorised insurer must understand and document what services the insurance manager is, and more importantly is not, providing in relation to the authorised insurer's obligations under the Code. This should be considered at the outset of the relationship and be included as part of the agreement between the authorised insurer and insurance manager. The services/document should also be reviewed on a regular basis.

3.3 Diagram 3



3.4 The role of the MLRO and DMLRO

Both the authorised insurer and the insurance manager, as relevant persons for the purposes of the Code, must appoint a Money Laundering Reporting Officer ("MLRO") and Deputy Money Laundering Reporting Officer ("DMLRO") as per paragraphs 23 and 24 of the Code, to exercise the reporting functions under paragraphs 25 and 27 of the code. They must both, establish, record, maintain and operate appropriate reporting procedures and controls to enable internal and external disclosures to be made.

The authorised insurer, and the insurance manager (where applicable), can meet their obligations in relation to the reporting procedures of the MLRO by:

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

3.5 External disclosures

For the avoidance of doubt, both the authorised insurer and the insurance manager are required to make an external disclosure where an insurance manager is providing services to an authorised insurer and the insurance manager detects suspicious activity in relation to the authorised insurer's customer. In practice the insurance manager may be providing all

services to the authorised insurer, including the MLRO; in these cases it is acceptable for one external report to be submitted on behalf of both the authorised insurer and the insurance manager. In such circumstances the external disclosure should clearly state in the grounds section that it is being made on behalf of both the authorised insurer and the insurance manager.

Where a managed authorised insurer detects suspicious activity by or within the insurance manager, and the insurance manager provides the manager authorised insurer's MLRO, this suspicion should be reported by the managed authorised insurer directly to the IOMFIU.

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

4. Paragraph 20 – Insurance exemptions

20 Insurance

(1) This paragraph applies to —

(a) an insurer; and

(b) an insurance intermediary.

(2) An insurer or insurance intermediary need not comply with Part 4 if the contract of insurance is a contract where —

(a) the annual premium is less than €1,000 or the single premium, or series of linked premiums, is less that €2,500; or

(b) there is neither a surrender value nor a maturity (for example, term insurance).

(3) In respect of a contract of insurance satisfying sub-paragraph (2) an insurer or insurance intermediary may, having paid due regard to the risk of ML/FT, consider it appropriate to comply with Parts 4 and 5 (if applicable) but to defer such compliance unless a claim is made or the policy is cancelled.

(4) If —

(a) a claim is made under a contract of insurance that has neither a surrender value nor a maturity value (for example on the occurrence of an insured event); and

(b) the amount of the settlement is greater than €2,500,

the insurer or insurance intermediary must identify the customer or claimant and take reasonable measures to verify the identity using reliable, independent source documents, data or information.

(5) An insurer or insurance intermediary need not comply with sub-paragraph (4) if a settlement of the claim is to —

(a) a third party in payment for services provided (for example to a hospital where health treatment has been provided);

(b) a supplier for services or goods; or

(c) the customer where invoices for services or goods have been provided to the insurer or insurance intermediary,

and the insurer or insurance intermediary believes the services or goods to have been supplied in respect of the insured event.

(6) If —

(a) a contract of insurance is cancelled resulting in the repayment of premiums; and

(b) the amount of the settlement is greater that €2,500,

the insurer or insurance intermediary, must comply with Parts 4 and 5 (if applicable).

(7) Sub-paragraphs (2), (3) and (5) do not apply if —

(a) the customer is assessed as posing a higher risk of ML/FT; or

(b) the insurer or insurance intermediary has identified any suspicious activity.

(8) If the insurer or insurance intermediary has identified any suspicious activity the relevant person must make an internal disclosure.

Paragraph 20 of the Code allows an insurer or insurance intermediary to either not undertake the requirements of Parts 4 and 5 of the Code (if applicable) or to defer such compliance provided certain criteria are met. The insurer must ensure appropriate monitoring takes place where any exemptions are used so that they are able to identify if these criteria are no longer being met.

Paragraph 20 only exempts an insurer or insurance intermediary from the requirements of Parts 4 and 5 of the Code (if applicable). The requirement under paragraph 6 of the Code to conduct a risk assessment for each customer always applies, although the Authority does recognise that relevant persons utilising the concession provided by paragraph 20 will have less detailed customer information upon which to base their risk assessments. Paragraph 6 includes the requirement for relevant persons to consider the risk factors included in paragraph 15(5) and (7) of the Code, which includes (at 15(7)(e)) consideration that a business relationship or occasional transaction with a politically exposed person ("PEP") may pose a higher risk of ML/FT. Relevant persons may be able to identify that their customer or prospective customer is a PEP without carrying out the screening required by paragraph 14 (which is in Part 5 of the Code), and if this is the case the individual's PEP status must be considered as part of the customer risk assessment.

Type of business	What CDD is required?
Annual single premium is less than €1,000 or Series of linked premiums is less than €2,500	• Could use paragraph 20(2) and not comply with Part 4 (apart from paragraph 13) • Could use paragraph 20(3) and defer compliance with Parts 4 and 5 unless a claim is made or the policy is cancelled • Can't use paragraph 20(2) or (3) if the customer is assessed as posing a higher risk of ML/FT • Can't use paragraph 20(2) or (3) if suspicious activity is identified
Annual single premium is more than €1,000 or Series of linked premiums is more than €2,500	• Paragraph 20 does not apply and Parts 4 and 5 (if applicable) must be complied with in full
No surrender or maturity value	• Could use paragraph 20(2) and not comply with Part 4 (apart from paragraph 13) • Could use paragraph 20(3) and defer compliance with Parts 4 and 5 unless a claim is made or the policy is cancelled • Can't use paragraph 20(2) or (3) if the customer is assessed as posing a higher risk of ML/FT • Can't use paragraph 20(2) or (3) if suspicious activity is identified
Surrender value or maturity value	• Paragraph 20 does not apply and Parts 4 and 5 (if applicable) must be complied with in full

Type of payment	What CDD is required?
Amount of settlement of less than €2,500 under a contract of insurance that has neither a surrender value nor a maturity value	• No CDD is required to be undertaken, as per paragraph 20(4) • Can't use paragraph 20(4) if the customer is assessed as posing a higher risk of ML/FT • Can't use paragraph 20(4) if suspicious activity is identified
Amount of settlement of more than €2,500 under a contract of insurance that has neither a surrender value nor a maturity value	• CDD is required to be undertaken, as per paragraph 20(4)

Settlement paid to: (a) A third party in payment for services provided; (b) A supplier for services or goods; or (c) The customer where invoices for services or goods have been provided	• No CDD is required to be undertaken, as per paragraph 20(5) • Can't use paragraph 20(5) if the customer is assessed as posing a higher risk of ML/FT • Can't use paragraph 20(5) if suspicious activity is identified
Cancellation of a contract of insurance resulting in an amount of settlement of less than €2,500	• No CDD is required to be undertaken, as per paragraph 20(6) • Can't use paragraph 20(6) if the customer is assessed as posing a higher risk of ML/FT • Can't use paragraph 20(6) if suspicious activity is identified
Cancellation of a contract of insurance resulting in an amount of settlement of more than €2,500	• Parts 4 and 5 (if applicable) must be complied with, as per paragraph 20(6)

Where the customer has been assessed as posing a higher risk of ML/FT paragraph 20(7) of the Code disapplies paragraphs 20(2), (3) and (5), which give the exemptions. Therefore, the insurer or insurance intermediary must undertake the requirements of Part 4 and 5 of the Code and cannot defer them.

If there is suspicious activity identified, the concession no longer applies, an internal disclosure must be made and the insurer or insurance intermediary must undertake the requirements of Part 4 of the Code. Also, ECDD should be undertaken in line with paragraph 15, unless the insurer or insurance intermediary reasonably believes conducting ECDD will tip off the customer.

5. Risk guidance

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

- a business risk assessment (paragraph 5)
- a customer risk assessment (paragraph 6)
- a technology risk assessment (paragraph 7)

These are key mandatory requirements under the Code, and need to contain detailed evidence to show the relevant person knows the risks faced and how the relevant person considered those risks as well as their mitigation. They are vital elements to show how a relevant person meets their Code obligations to try to prevent money laundering or terrorist financing being effected through their business.

The non-life insurance sector is broad and the ML/FT risks will vary for each business based on a wide range of factors such as the types of products and services they supply, their customers and delivery channels.

There are a number of different types of business in this sector, therefore this document covers some of the general risk factors common to the sector as a whole and then focusses on particular individual business types where necessary.

In order to complete the required risk assessments and keep them up-to-date vigilance should govern all aspects of an entity's dealings with its customers, including:

- onboarding;
- customer instructions;
- ongoing monitoring of the business relationship;
- payments out/settlement/third party settlement/assignments; and
- technology/security issues if there is an online element to the business relationship.

As noted above (and detailed in diagrams 1, 2 and 3) both the authorised insurer and the insurance manager as relevant persons for the purposes of the Code each must prepare an assessment of its exposure to ML/FT risk - this includes a Business risk assessment ("BRA"), and an assessment of the risk of ML/FT that a business relationship or one-off transaction poses for each of its customers (the Customer risk assessment ("CRA")).

The requirement of paragraph 6(3)(b) of the Code for the CRA to consider the nature, scale, complexity and location includes considering the specific activity that is being insured. This may require looking through arrangements (e.g. looking through a fronting insurer and considering the risks of the specific activity they are insuring).

A Technology risk assessment ("TRA") must also be carried out by each relevant person. If it is considered that there is no technology risk (either for the authorised insurer or the insurance manager) the considerations and conclusion should still be documented. The authorised insurer's TRA may be similar, or based upon, the TRA of its insurance manager. However, the authorised insurer must have its own distinct TRA, and clear consideration of the authorised insurer's own technological risk must take place.

It is common that an authorised insurer will delegate the completion of its BRA, TRA and its CRAs to its insurance manager. If this is the case this should be clearly documented in the agreement which sets out each party's responsibilities. Regardless of any outsourcing or delegation that takes place, the ultimate responsibility for ensuring compliance with the Code remains that of the relevant person.

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.

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

5.1 General higher risk indicators

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

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

As stated in paragraph 13 of the Code:

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

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

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

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

This list of higher risk indicators is by no means exhaustive, and relevant persons should be vigilant for any transactions where suspicion may be aroused and take appropriate measures.

- Applications from potential customers in jurisdictions where a comparable product could be provided "closer to home" and the reason for choosing the Isle of Man cannot be understood.
- Being asked to insure something that is not insurable, and where the rationale for the insurance cannot be understood.
- Customers looking to take out policies with values that appear inconsistent with their insurance needs.

- The customer acts in a hurry, does not analyse an offer, is not interested in charges and costs, chooses the most expensive offer, which may not be the most appropriate one.
- Acceptance of premiums that appear to exceed the customer's means or very unfavourable provisions or riders.
- Difficulties and delays in gaining CDD information and documentation.
- The relationship is controlled by a third party, or there are multiple indicators of third party deposits or payments.
- Overpayment of premiums and unwillingness to take it for a next premium instalment.
- One or several overpayments of the policy followed by requests that any reimbursement be paid to a third party.
- A natural person paying premiums from the account of a legal person.
- Multiple payments of premiums from different accounts that do not exceed a reportable threshold.
- Atypical incidence of pre-payment of premiums.
- Large cash or other forms of anonymous transactions.
- Cancellation and request for the refund to be paid to a third party.
- Requests to cancel the insurance policy without a valid explanation.
- Unconditional acceptance of a lower amount of reimbursement.
- Reimbursement in a currency different to the original premium.
- Apparently legitimate claims which occur with abnormal regularity.
- A change of ownership/assignment of a policy just prior to a loss occurring.
- Claims requested to be paid to persons not naturally associated with the claim.
- Claims requested to be paid to persons other than the insured or third parties.
- Withdrawal of a claim when an insurer requests additional information.
- Transactions involving undisclosed parties.
- Customer places an unusual emphasis on the necessity for secrecy.
- Use of intermediate corporate vehicles or other structures that have no apparent rationale, that unnecessarily increase the complexity of ownership, or otherwise result in a lack of transparency.
- The company has new ownership and the background and appearance of the new owners does not harmonise with the company profile, or the financial activities of the customer suddenly changes after the change of ownership.
- Customers that are legal entities whose structure makes it difficult to identify the ultimate beneficial owner.
- Sudden changes in the activity of the customer that are unusual and not in line with their known profile.

5.2 Higher risk matters

Paragraph 15(5) of the Code mandates certain circumstances where a customer must be assessed as posing a higher risk. Apart from these matters the Authority does not generally mandate which customer or sectors must be viewed as higher risk. The Authority does not

have any objection to a regulated entity having higher risk customers provided that they have been adequately risk rated in accordance with the regulated entity's procedures and any mitigating factors have been documented.

As per paragraph 15(3) of the Code relevant persons must conduct Enhanced Due Diligence where a customer has been assessed as posing a higher risk of ML/FT.

Further information about the customer risk assessment and the treatment of higher risk customers can be found in the Handbook.

6. Kidnap, ransom and cyber insurance

The payment of a ransom (whether paid in fiat or virtual currencies generates proceeds of crime), and these proceeds may be used for terrorist of proliferation financing. The FATF report into Organised Maritime Piracy and Related Kidnapping for Ransom (2011) notes that when there is advanced notification to the relevant authority of a ransom payment this can greatly assist in the investigation. Conversely, when payments are not reported this can make it difficult to track the funds and determine how they are laundered or used, especially if the ransom is paid in cash. It is important that registered persons comply with the Code requirements in relation to external disclosures if they are involved in a ransom payment. Relevant persons should be aware that the payment of a ransom is illegal in some jurisdictions.

7. Assignments and transfer of ownership

When a policy is assigned the assignee becomes the customer and the requirements of Part 4 and 5 of the Code (if applicable) must be complied with.

8. Cooling off/cancellation periods

Where a customer takes up the right to decline to proceed with a contract during a cooling off or cancellation period (where this is permitted by the prevailing regulations and rules under which the contract was sold), the circumstances surrounding the request to cancel must be considered and if they are viewed as suspicious then this suspicion must be reported. That being the case, suspicion reporting procedures should be followed as set out in chapter 5 of the Handbook.

Further information about making payments out can be found at section 10 of this document.

9. Beneficial Ownership and control

The Code's definition of beneficial owner differs from the definition in the Beneficial Ownership Act 2017 and the definition of controller in the Insurance Act 2008.

The requirements of paragraph 12 of the Code must be complied with regardless of the size of structure that the customer is a part of. Guidance regarding complying with the beneficial ownership and control requirements of the Code can be found in the AML/CFT Handbook.

10. Payments out

When making payments a relevant person should be mindful of the requirements of paragraphs 12(7) (below) and 20 (above) of the Code.

12 Beneficial ownership and control

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

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

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

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

Any payment out to a policyholder as a result of such a right being exercised should normally be to the source account from which the monies were originally sent. If the payment out is to be by cheque it should be payable to the policyholder and marked "account payee only".

Under certain circumstances payment may be made to a third party account, for example a client money account, or payment to the original account may be impossible, for example if the account has subsequently been closed. In these circumstances an insurer must be satisfied with the connection between the payee and the policyholder, and must also consider whether the payment request is suspicious, in which case, suspicion reporting procedures must be followed as set out in chapter 5 of the Handbook.

Whenever payments are made relevant persons must be mindful of requirements regarding sanctioned individuals and entities. The Isle of Man Customs and Excise Division has issued guidance regarding sanctions.