ISLE OF MAN
FINANCIAL SERVICES AUTHORITY

Lught-Reill Shirveishyn Argidoil Ellan Vannin

JULY 2024

ACCOUNTING PROFESSION

CUSTOMER RISK ASSESSMENT

THEMATIC REPORT

www.iomfsa.im

aml@iomfsa.im

Contents

Colour key used in this document:

AML/CFT Code 2019

AML/CFT Handbook

AML/CFT CRA Thematic Data

Best Practice

1 Glossary of terms

TERM	MEANING IN THIS REPORT
Accounting profession	External accountant, tax adviser and/or payroll agent registered businesses
AML/CFT	Anti-Money Laundering/Countering the Financing of Terrorism
Authority	The Isle of Man Financial Services Authority
BRA	Business Risk Assessment
CDD	Customer Due Diligence
Code	Anti-Money Laundering/Countering the Financing of Terrorism Code 2019
CRA	Customer Risk Assessment
DNFBP	Designated Non-Financial Businesses and Professions
ECDD	Enhanced Customer Due Diligence
FC	Financial Crime
Handbook	Anti-Money Laundering/Countering the Financing of Terrorism Handbook
HNWI	High Net Worth Individual
Licenceholder	Licensed Entities
ML/FT	Money Laundering/Financing of Terrorism
NPO	Non-Profit Organisation
NRA	National Risk Assessment
PEP	Politically Exposed Person
PF	Proliferation Financing
Relevant Person	Means a person carrying on business in the regulated sector included in paragraphs 2(6)(a) to (t) of Schedule 4 to the Proceeds of Crime Act 2008
Registered Person	Means a person registered under section 9 of the Designated Businesses (Registration and Oversight) Act 2015
Regulated	Refers to firms regulated under the Financial Services Act 2008, the Insurance Act 2008, and the Retirement Benefits Schemes Act 2000
TRA	Technology Risk Assessment

2 Background

2.1 Executive Summary

The Authority has completed a thematic project involving external accountant, tax adviser and payroll agent ("accounting profession") registered businesses on the Island. The Authority, using existing and known data and information on external accountant, tax adviser and payroll agent registered businesses, concluded a thematic project would be valuable to further connect and work with the sector.

This project has allowed and enabled the Authority to gather further data, assisting in risk assessing both the firms and sector itself, as well as building knowledge and findings to feedback into the Handbook, the AML/CFT sector specific guidance documents and the NRA.

The Authority's regulatory objectives are:

- securing an appropriate degree of protection for policyholders, members of retirement benefits schemes and the customers of persons carrying on a regulated activity.
- the reduction of financial crime; and
- the maintenance of confidence in the Island's financial services, insurance, and pensions industries through effective regulation, thereby supporting the Island's economy and its development as an international financial centre.

A key part in achieving these objectives is the Authority's oversight and supervisory function, which encompasses undertaking supervisory inspections.

The planning for the thematic began in early 2023 and the background was shared in a press release issued on the Authority's website on 19 July 2023. The thematic project consisted of one phase, carrying out desk-based inspections and analysis regarding CRAs and the associated procedures and controls.

The CRA desk-based inspections commenced in July 2023, 51 desk-based inspections were carried out by the Authority of registered persons in the accounting profession. The Authority's focus included the CRAs (paragraph 6 of the Code), procedures and controls (paragraph 4 of the Code) of these firms to assess their compliance with these areas of the Code.

The project concluded in April 2024, with an individual inspection report issued to each of the 51 firms inspected. This overarching report outlines the results from the thematic project, highlighting some learning points and areas of best practice.

A relevant person's CRAs, CRA procedures and controls are vital to evidence their understanding of the risks which their customers may pose to the firm's business. Additionally, robust fit-for-purpose CRAs allow firms to identify those customers with higher risk profiles, in order to apply appropriate procedures and controls in order to prevent ML, FT, PF and FC. Relevant persons should consider whether each risk factor recorded within the CRAs should be calibrated or weighted differently, dependent on how the relevant person assesses each of the various factors. Further, the CRA exercise is crucial in order for firms to adequately resource their monitoring of customers as part of a risk-based approach.

We hope this report will assist firms in assessing their ML/FT risks when reviewing and/or updating their CRA and any associated procedures and policies. We would like to thank the firms involved in participating in the completion of this thematic.

Robust CRAs allow firms to identify customers with higher risk profiles

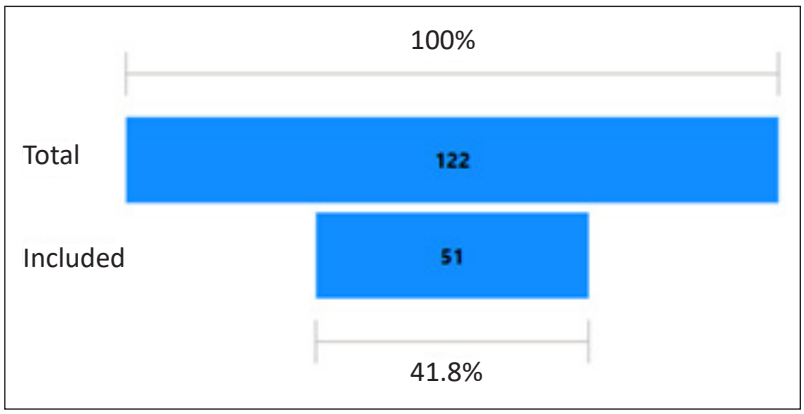
2.2 Thematic Scope

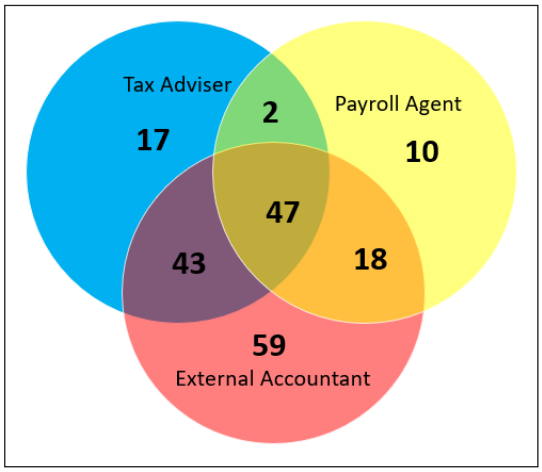
Initially, the project consisted of reviewing and analysing existing data held by the Authority from all 196 accounting profession firms registered under the Designated Businesses (Registration and Oversight) Act 2015 at the time of the planning exercise.

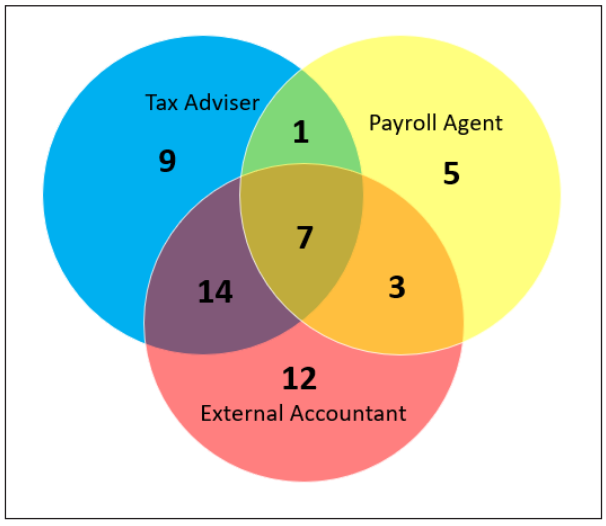
For the purpose of this thematic project the accounting profession includes registered persons undertaking and carrying out external accountant, tax adviser or payroll agent designated business activity.

Of the 196 firms, 74 have chosen to be overseen by a delegated body (such as the ACCA[1], ICAEW[2] or the IFA[3]), resulting in 122 accounting profession firms being overseen by the Authority for AML/CFT.

A total of 51 firms, or 41.80% of the accountancy professionals supervised by the Authority, were selected to participate in the thematic.



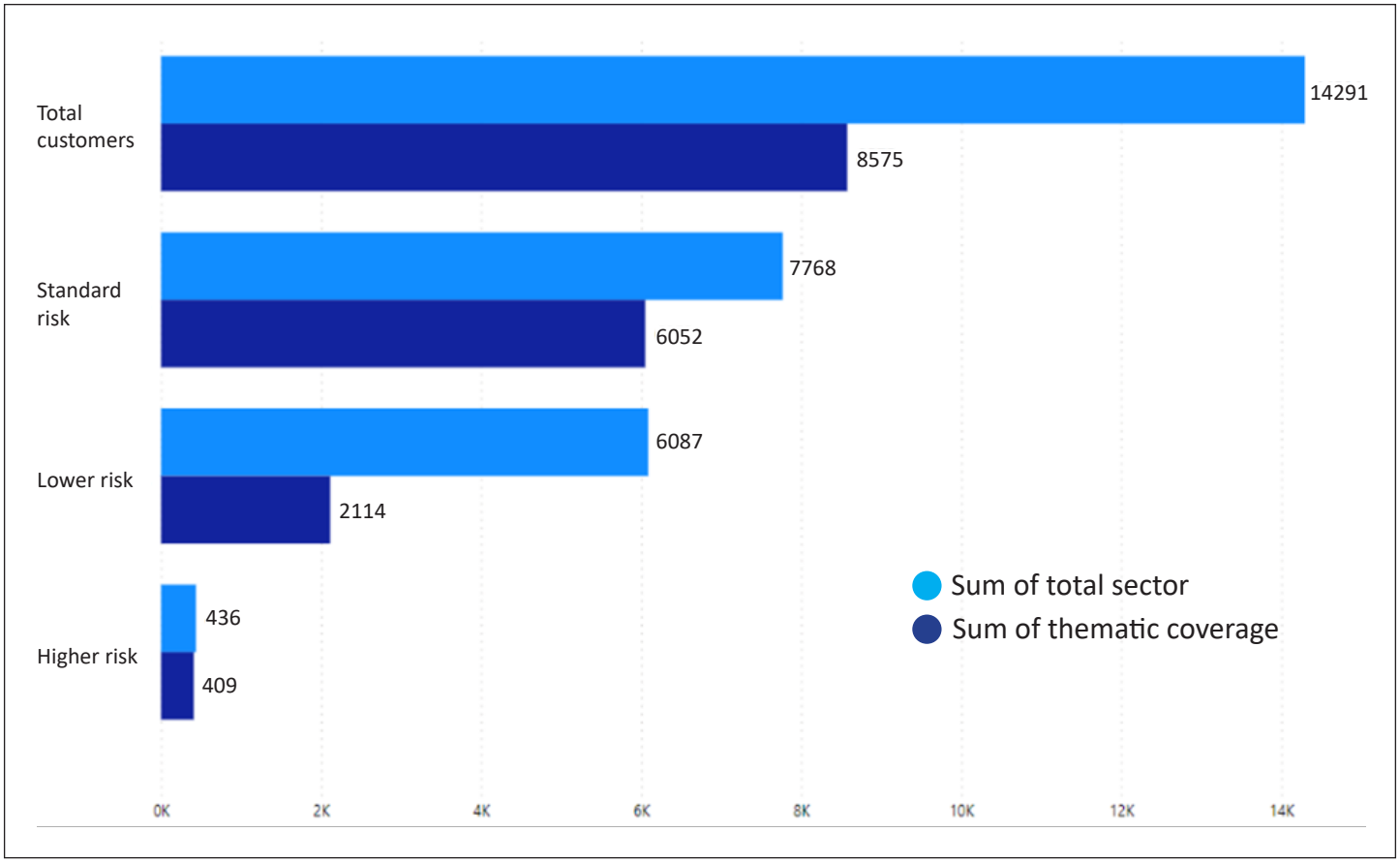




Of the 122 accounting professionals the Authority inspected 51 registered persons, their registerable activity included the following, which totalled[4]:

- External Accountants – 36
- Tax Advisers – 31
- Payroll Agents – 16

[1] Association of Chartered Certified Accountants
[2] Institute of Chartered Accountants for England & Wales
[3] Institute of Financial Accountants
[4] Please note that registered persons may carry out, as notified as part of any registration with the Authority, a number of activities listed included in paragraphs 2(6)(a) to (t) of Schedule 4 to the Proceeds of Crime Act 2008



The Authority operates a risk-based approach to supervision, therefore the Authority dedicated more resource to reviewing higher risk customers as part of the CRA thematic. The collective customer base of firms inspected in comparison of the sector comprise:

- **93.81%** of the higher risk customers;
- **77.91%** of the standard risk customers; and
- **34.73%** of the lower risk customers.

60% of the total customer base of the accountancy profession firms supervised by the Authority were captured in this thematic exercise.

The thematic exercise has given the Authority a stronger understanding and overview of the sector and has enabled the identification of trends.

Best practice and poor practice observations relating to CRAs and CRA procedures will feedback into the guidance framework to benefit all relevant persons in relation to their compliance with the Code.

The thematic exercise has given the Authority a stronger understanding and overview of the sector

2.3 AML/CFT Code 2019 - CRA Obligations

Paragraph 6 of the Code

6 Customer risk assessment

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

(2) The 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;

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

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

(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) and 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.

The Code sets out the minimum legal obligations for relevant persons to establish, maintain and operate procedures that have regard to the materiality of ML/TF/PF risk posed by the customer.

Paragraph 6 of the Code requires that a relevant person must carry out a CRA that estimates the ML/TF/PF risks posed by the customer. The Authority's AML/CFT Handbook also provides information to help relevant entities consider their obligations, with section 2.2.9 offering further guidance on carrying out CRAs required under the Code.

It is important to note that where the Code refers to a relevant person estimating the risk of FT, this should also include the financing of proliferation, as prescribed in paragraph 3 of the Code, 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.

The Authority's AML/CFT Handbook provides further guidance on CRAs

Handbook quote

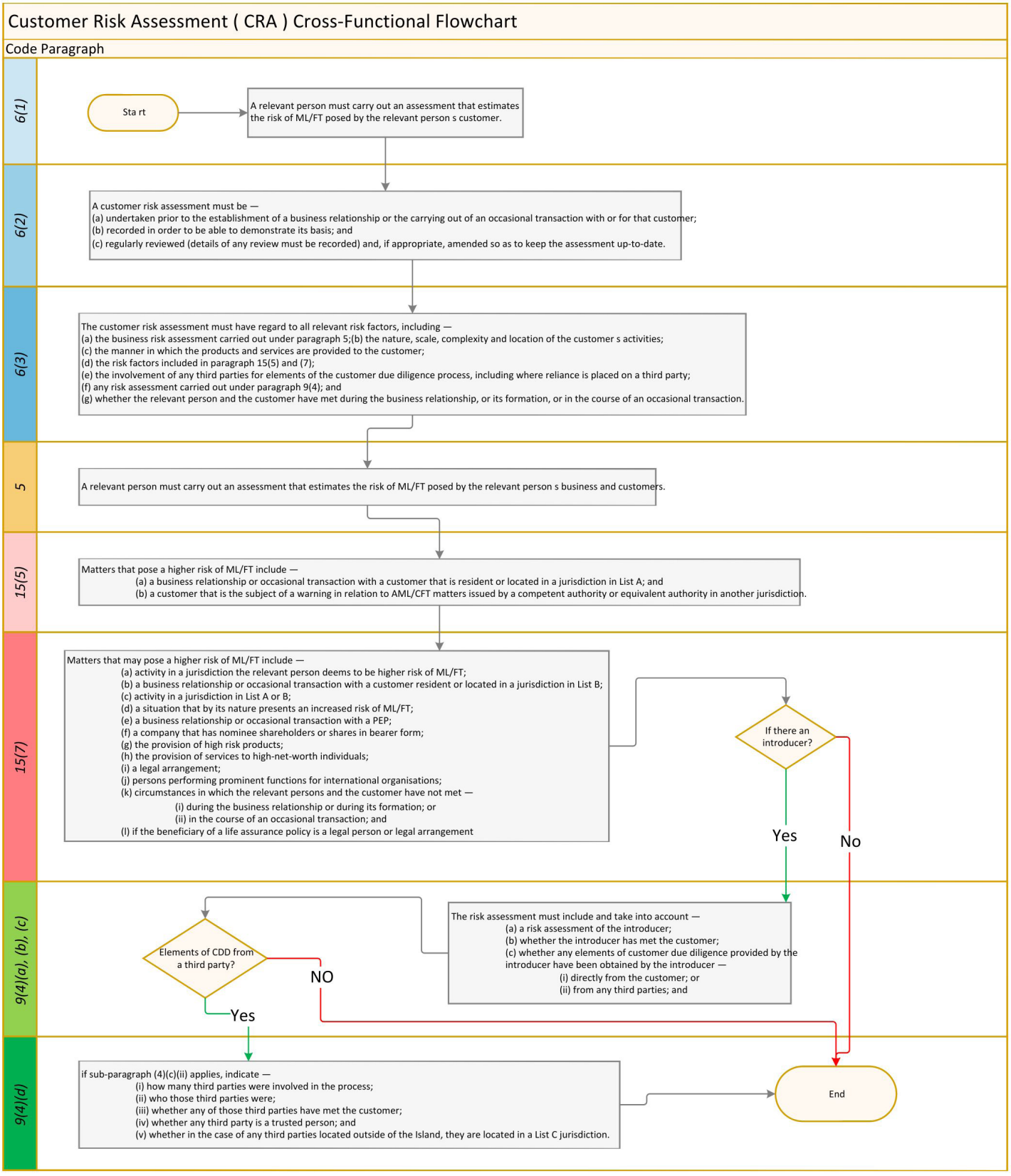
2.2.9 Customer risk assessment

Relevant persons should note that assessing a customer as higher ML/FT risk does not automatically mean a customer is a money launderer or is financing terrorism. Similarly, assessing a customer as low ML/FT 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 risk and the relevant person complies with the ECDD requirements and restrictions on exemptions and simplified measures within the Code.

Good practice in relation to conducting CRAs includes ensuring:

- CRAs are clearly recorded and undertaken in a timely manner.
- CRAs are reviewed regularly and in accordance with internal procedures and controls.
- CRA reviews are clearly documented.
- CRAs have regard of all risk factors prescribed in the Code; and
- CRAs also have regard of any additional risk factors that are unique to the particular business and each customer's circumstances.

The Code sets out the minimum legal requirements and risk factors to assess when estimating the risk of ML/FT/PF of a customer. As set out in paragraph 6 of the Code, firms must consider a multitude of risks defined within paragraphs 5, 6, 9 and 15 of the Code. Please see below a high-level example flowchart/process map for carrying out a CRA in line with the Code.



3 Phase 2 - CRA Inspections

3.1 Scope

The primary objective of the CRA accounting profession thematic project was to review a sample each firm's CRAs and CRA documentation, to determine whether the firm had demonstrated the requirements of the Code. The four main objectives of the desk-based inspections included the following:

- **Objective 1:** Review the procedures and controls considering paragraph 4 of the Code.
- **Objective 2:** Review the customer risk assessment considering paragraph 6(1) of the Code.
- **Objective 3:** Review the customer risk assessment considering paragraph 6(2) of the Code.
- **Objective 4:** Review the customer risk assessment considering paragraph 6(3) of the Code.

As part of this thematic inspection process, the firms involved were given five working days to supply the requested documentation to demonstrate and evidence compliance with the inspection's scope and objectives in line with the Code.

The Authority's officers reviewed and assessed compliance with the Code examining firms CRA templates, the relevant policies, procedures or guidance documents regarding the CRA. With regards to the CRA the Authority selected up to five customers most recent CRAs.

In considering the procedure level and risk assessment level the Authority were able to establish the selected firms' level of compliance with paragraphs 4 and 6 of the Code.

The customer file selection process requested firms to provide copies of the CRAs for:

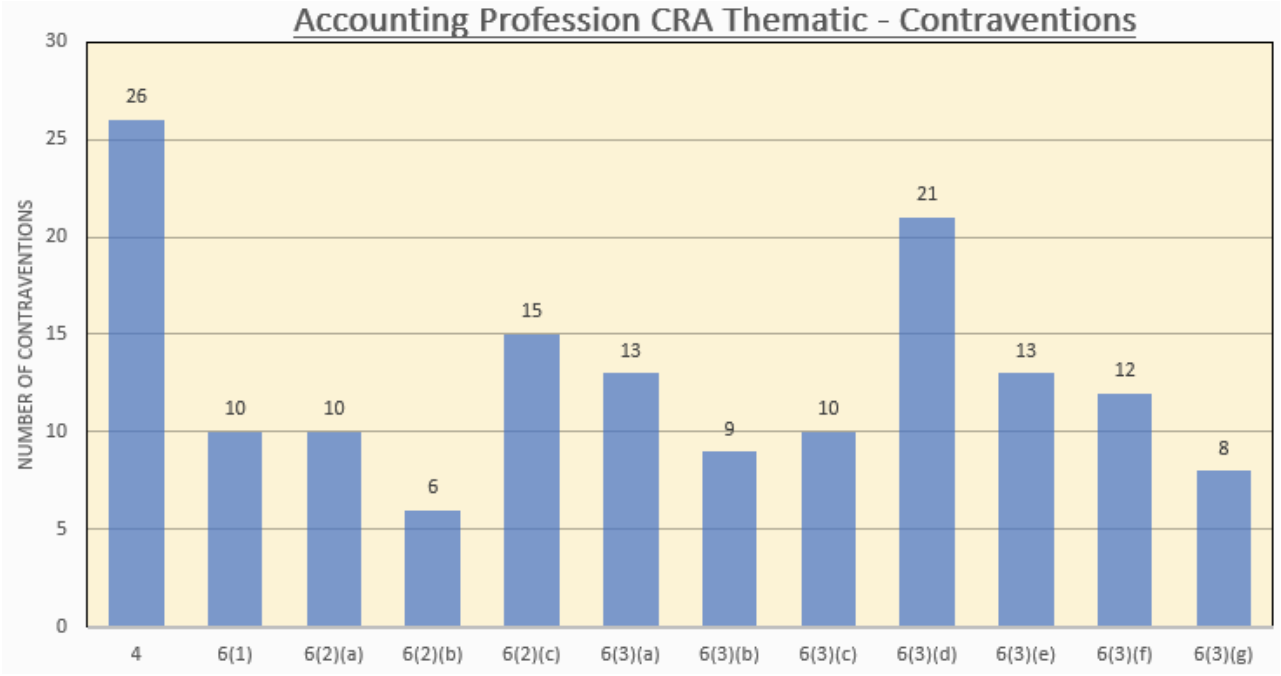
- **Oldest** customer;
- **Newest** customer;.
- **Highest Risk** customer;
- **Highest Income** customer; and a
- **PEP** customer.

If any of the requested customer file(s) were not applicable, repeated, duplicated or already covered by a previous requested customer file, a replacement customer file of the next highest risk customer was selected.

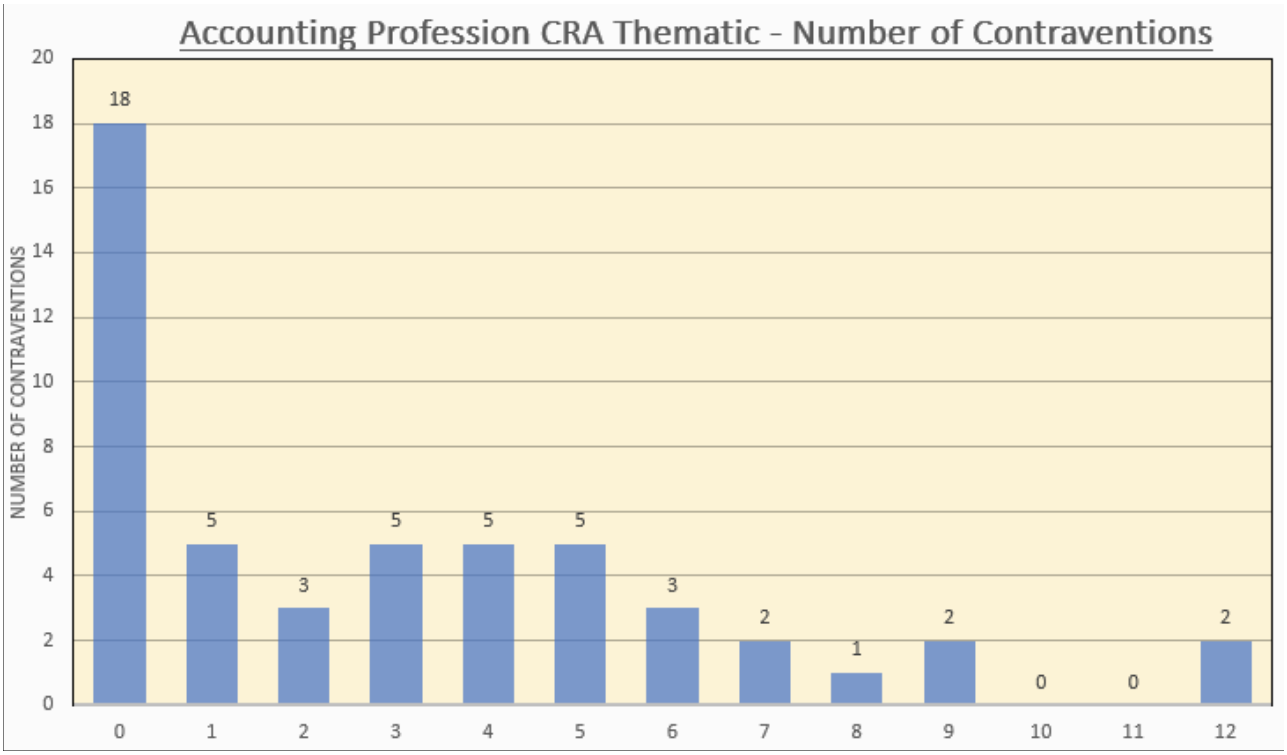
3.2 Overall Results and Key Findings

Detailed analysis of the results and outcomes from the thematic project in relation to paragraphs 4 and 6 of the Code are analysed within sections 3.3 and 3.4 of this report.

Following analysis of the outcomes from the CRA inspection reports, and considering the type of contraventions identified, the Authority has noted that out of the total 51 inspections, the three most common contraventions identified were paragraphs 4, 6(2)(c) and 6(3)(d) of the Code, as highlighted below.



Overall, out of the 51 inspections, 26 of firms inspected had zero or fewer than two specific Code paragraph contraventions identified.



3.3 Key Findings: Paragraph 4 of the Code

3.3.1 Paragraph 4 of the Code

Paragraph 4 of the Code

4 Procedures and controls

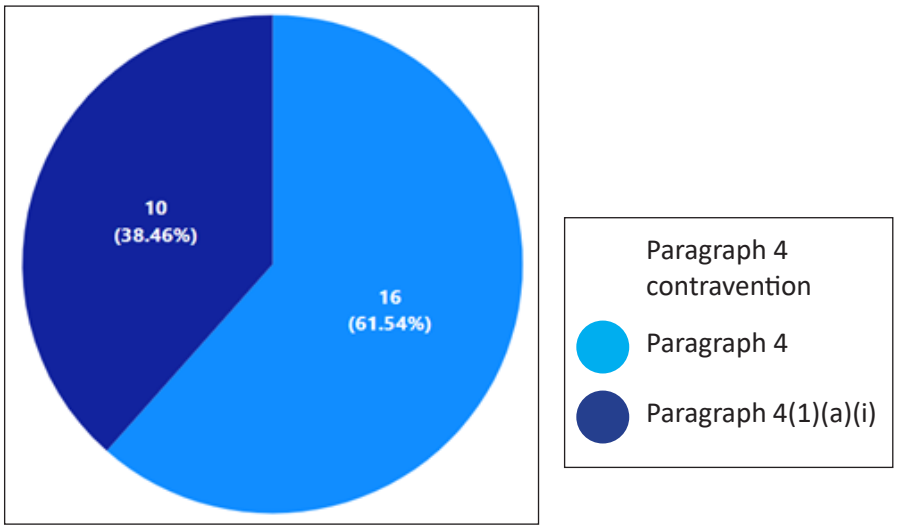
(1) A relevant person must not enter into or carry on a business relationship, or carry out an occasional transaction, with or for a customer or another person unless the relevant person.

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

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

49%
Compliance with paragraph 4 of the Code

The first objective of the inspections was to consider paragraph 4 of the Code. The Authority's officers observed mixed levels of compliance in relation to this paragraph of the Code, with approximately half of firms inspected having a contravention identified. There were various levels of contraventions of paragraph 4 of the Code, with some firms having isolated findings within paragraph 4 (such as 4(1)(a)(i) of the Code) and other firms with recorded contraventions across the entirety of paragraph 4 of the Code.



Those specific contraventions of paragraph 4(1)(a)(i) of the Code totalled 38.46% of the identified paragraph 4 contraventions, which were mostly the result of isolated instances of a failure to correctly operate, record or maintain CRAs and CRA procedures and controls within the firm.

Whereas contraventions of paragraph 4 of the Code in its entirety amounted to 61.54% of the total identified paragraph 4 contraventions seen above, wherein firms were found to not have established or established sufficient CRA procedures and controls. As a result these firms were not able to evidence compliance with paragraph 4. Material contraventions are recorded by the Authority, where firms do not have formal written, documented procedures and controls in relation to CRAs. The Authority would like to reiterate that all regulated and registered persons must have documented procedures and controls that are established, recorded, operated, and maintained in order to comply with each paragraph within Parts 3 to 9 of the Code.

Handbook quote

2.1.2 Procedures and controls

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 and the harm that crime, terrorism, and the proliferation of weapons of mass destruction present for wider society.

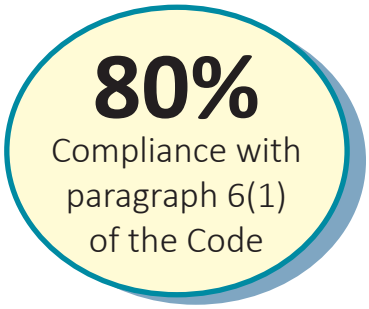
3.4 Key Findings: Paragraph 6 of the Code

3.4.1 Paragraph 6(1) of the Code

Paragraph 6(1) of the Code

6 Customer risk assessment

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



Handbook quote

2.2.9 Customer risk assessment

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.

Paragraph 6(1) in context

The second objective of the inspections was to consider paragraph 6(1) of the Code. The main objective of a CRA is to estimate the risk of ML/FT/PF posed by the relevant person's customer(s).

Firms should decide on the most appropriate way to estimate ML/FT/PF risk in a robust manner, 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 they are exposed by their customers.

Below are some common questions and risks the accountancy sector may wish to include considering within their CRAs. The Accountants and Tax Advisors Sector Specific AML/CFT Guidance Notes August 2021 and the Payroll Agents Sector Specific AML/CFT Guidance Notes September 2021 both contain further guidance on this topic.

Country/geography/location risk

- The nature of the customer's activities?
- Is the nature of the customer one that could be considered inherently higher risk?
- The scale of the customer's activities?
- Turnover, revenue, volume of transactions?
- The complexity of the customer's activities?
- The location of the customer's activities?
- Activity in a jurisdiction in List A or B?

Customer risk

- Has negative or adverse media been identified in relation to the customer?
- Is the customer a PEP?
- Is the customer a HNWI?
- Is the customer a legal person (i.e. a company or trust)?
- Is the customer performing prominent functions for international organisations?
- Is the customer the subject of a warning in relation to AML/CFT matters issued by a competent authority or equivalent authority in another jurisdiction?
- Does the customer have links to sectors that involve significant amounts of cash?
- Has there been a material change to the accounts from the expected nature and purpose?

Transaction/service and associated delivery channel risk

- The manner in which the products and services are provided to the customer?
- Services or products offered (any high-risk products)?
- Has the customer been met?
- Is this a one-off transaction?
- Was a third party or introducer involved in the relationship?

When estimating the risks, relevant persons may find it helpful to use various risk scoring / rating classifications both for the customer(s) and for the individual factors contributing to the assessment of the customer's risk profile, for example, the risk factors prescribed in paragraph 6(3) of the Code. However, it must be remembered 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.

Relevant persons should consider risk factors beyond those specified in the Code, relevant persons should always make efforts to determine the risk factors that are relevant to their customers' circumstances.

Classifications for ML/FT/PF risks assist firms in developing their assessments to understand how to manage risks, how risks may relate to each other, the prioritising and communicating of risks, and can be useful in informing a firm's allocation of resources when mitigating those risks. Appropriate risk ratings also enable relevant persons to determine whether the use of Code concessions is permissible.

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, with appropriate narrative, which demonstrates understanding.

Paragraph 6(1) observations

The Authority's officers observed a range of formats, practices and methodologies used to estimate customer risk across accountancy profession. Although the Authority does not recommend one particular approach, relevant persons should, in all cases, clearly document and explain the method used, and ensure the outcomes are understood. Some approaches were simpler, and others were more complex with multiple layers of analysis and reasoning; this range reflects the fact that the nature, scale, and complexity of each firm is different.

Using a calculated risk rating methodology will allow firms to accurately assess separate risk factors in a given customer's situation, increasing the firm's understanding of priority and urgency. Additionally, using and applying different weightings when calculating overall specific risk factors or risk sections is an advanced and useful tool in risk management and evaluation.

Example CRA Risk Methodology

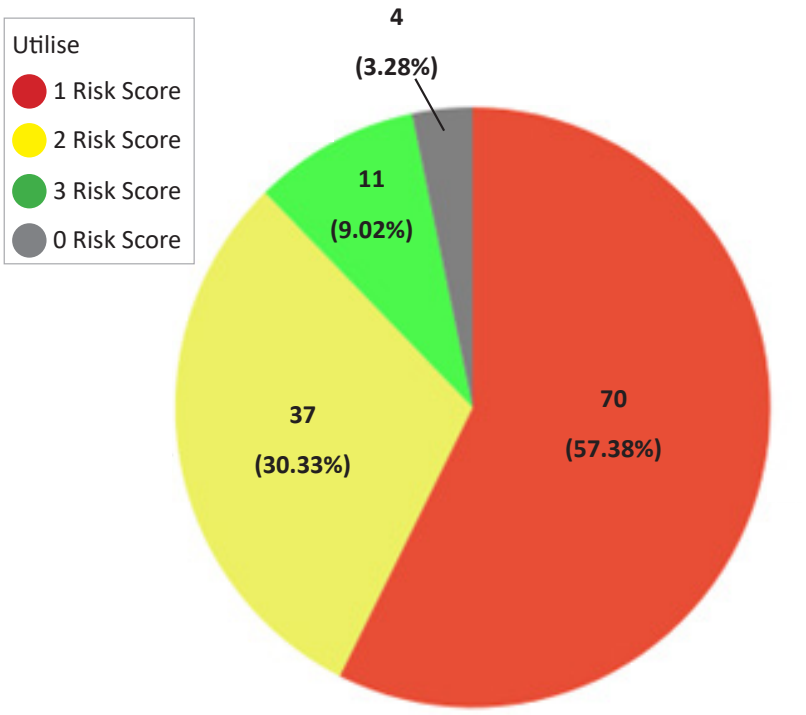
Sections / Questions	Section Weighting	Risk Scoring						Total Score
		0	1	2	3	4	5	
Section 1	8	0	8	16	24	32	40	
Section 2	2	0	2	4	6	8	10	
Section 3	4	0	4	8	12	16	20	
Section 4	5	0	5	10	15	20	25	
Section 5	5	0	5	10	15	20	25	
Section 6	6	0	6	12	18	24	30	
Section 7	3	0	3	6	9	12	15	
Section 8	8	0	8	16	24	32	40	
Section 9	7	0	7	14	21	28	35	
Section 10	2	0	2	4	6	8	10	
Section 11	1	0	1	2	3	4	5	
Section 12	9	0	9	18	27	36	45	
Question 1	100	0					500	
Question 2	100	0					500	
Question 3	100	0					500	

CRAs that accurately estimate the ML/TF risk of a customer allow firms to target the highest risk customers to ensure they receive the right level of attention. This also allows for more efficient and effective resource allocation and future planning within the firm. The anonymised example shows a risk scoring methodology that was used to underpin the CRA.

The CRA was split into multiple sections, containing multiple questions, with each section given a risk weighting. Thereafter, responses and answers to questions within sections were assigned a scoring from 1 to 5, with the resultant score being multiplied by the weighting in order to give a total risk score outcome.

The CRA methodology also featured 'override' individual questions relating to particularly high-risk factors that were deemed unacceptable to the relevant person's risk appetite. Such questions were in their own section, bearing an individual section with an extreme weighting. As a result, a 'Yes' answer to any of these questions resulted in an unacceptable risk rating.

Establishing and maintaining a comprehensive and tailored risk rating methodology, as per the example, alongside clear policy and procedures, which explain the reasoning, approach and decisions taken, is a matter of best practice for demonstrating and evidencing compliance with the Code.



The number of risk ratings that were observed to be in use and utilised by the 122 firms were considered by the Authority. For the majority of firms, there was only one or two Code aligned risk scores (either; Lower, Standard or Higher) in use or applied to the customer base of a relevant person, with 57.38% using only one and a further 30.33% utilising two risk ratings.

It is noted by the Authority's officers, where permissible, firms' CRA templates, procedures and controls should be developed and encompassing of a range of risk ratings when assessing the customer base, where appropriate. Although, in certain scenarios and businesses, utilising all the three Code risk ratings inclusive of higher, may not be the norm, firms should have the ability and controls in place to access or manage these scenarios.

Limited or sole risk rating use may be a system of poor procedures and controls, ineffective risk methodology or inappropriate identification of higher risk factors as a standard or lower ML/FT risk. The Handbook provides further guidance on this matter in section 2.2.4.

Case Study 1:

In the case of one firm's CRA template and associated CRA procedure, the Authority's officers saw evidence of a detailed risk methodology featuring an extensive suite of risk factors, beyond those prescribed in the Code. With each customer considered on a case-by-case basis. The CRAs were in line with the documented procedure and the methodology of the CRAs was clearly explained, such that a new staff member could correctly operate the procedures and controls to assess a new customer's risk rating, with the resultant risk assessment giving an accurate picture of the overall risk presented by the customer.

In practice, questions, and sections of the CRA were accurate and detailed. Each risk section contained a calculation of the risks within the section, which were weighted appropriately, and the CRA thereafter concluded with a summary of the weighted risks and an overall risk rating of the risk posed by the customer. This effectively and concisely demonstrated to the Authority's officers why the firm believed the applied risk rating was suitable, and the calculation that had gone into the rating.

CRA Risk Methodology - Best Practice:

- Clearly documenting and implementing a considered and relevant matrix and methodology.
- Weighting of each risk factor considered.
- Considers more than just the risk factors prescribed in paragraph 6(3) of the Code.
- Includes a summary or conclusion of risk factors; and
- Results in a risk rating for that particular customer that assesses the overall threat of ML/FT based on the specifics of the customer's profile.

3.4.2 Paragraph 6(2) of the Code

Paragraph 6(2) of the Code

6 Customer risk assessment

(2) The 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.

(b) recorded in order to demonstrate its basis; and

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

Handbook quote

2.2.9.1 Timing of the CRA

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

The third objective of the inspections was to consider paragraph 6(2) of the Code. Overall, the Authority's officers observed fairly high levels of compliance in relation to paragraph 6(2) of the Code throughout the thematic.

In considering paragraph 6(2) of the Code, the Authority's officers also considered firms' compliance with paragraph 4(1)(a)(i) of the Code. A poor practice trend observed by the Authority's officers was firms stating in their own procedures and controls that the CRA would be reviewed and updated within a certain period. However, during the inspections the Authority's officers observed in some instances that a number of firms had only documented and evidenced reviews or updates of the CRA within a given calendar year, without providing a specific date. In such cases, reviews were seen to be ranging from up to 13 to 23 months apart (e.g. February 2022 to March 2023). This extended time gap between CRA reviews was not in-keeping with those relevant persons' documented procedures and controls, wherein the review period is defined as (at least) yearly. As a matter of best practice, firms should undertake and document scheduled, ad-hoc or triggered reviews, updates, and amendments to CRAs as the business, customers, or external risk factors develop and change.

The CRA and associated procedure(s) should consider and make use of data, findings and trends from the BRA and the relevant persons customers. The CRA and procedure should also document and describe the current controls, mitigations and considered risks that are featured in the methodology. As part of such a procedure it should document the options of overriding the risk rating of a CRA and the relevant sign-off process. The Authority expects that the Board or senior management sign-off and approve the CRA and associated procedure(s). This sign off is attestation that the firm consider the procedures to befit for purpose and commensurate with the risk profile of the business.

The business should include and use any new or improved aspects that have been adopted from the outcomes of concurrent TRAs and BRAs as part of any review or update to any CRA procedures. The sign-off and approval of the CRA procedure/methodology should be within the period specified moving forward and ensure regular reviews and any amendments are clearly documented in minutes and version controls.

Paragraph 6(2) - Best Practice:

- The initial CRA is clearly documented and dated, having been undertaken prior to the establishment of the business relationship or occasional transaction.
- Regular reviews are documented and evidenced in line with the relevant person's procedures and controls.
- All subsequent reviews of the CRA are separately recorded and not overridden (or the date updated).
- Includes clear details of the staff member(s) involved in completing and approving the CRA(s).
- CRAs are also carried out and updated on an ad-hoc basis, as and when risk factors occur from various local or global events (such as a jurisdiction's grey listing) that may affect AML/CFT or ML/FT risks posed by the customers to the business.

3.4.3 Paragraph 6(3) of the Code

Paragraph 6(3) of the Code

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.

Handbook quote

2.2.9.2 relevant risk factors including matters that pose or may pose higher ML/FT risks.

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 fourth objective of the inspections was to consider paragraph 6(3) of the Code. The Authority's officers saw mixed levels of compliance in relation to paragraph 6(3) of the Code throughout the thematic project; however, generally, more positive than negative outcomes were observed.

All of the risk factors prescribed in paragraph 6(3) of the Code must be fully considered, with such consideration assessed, and mitigated as appropriate with the analysis clearly articulated within the CRA. However, this list is not exhaustive, and firms should consider all relevant risk factors, even if not expressly included and prescribed in paragraph 6(3) of the Code.

Paragraph 6(3)(a) of the Code

6 Customer risk assessment

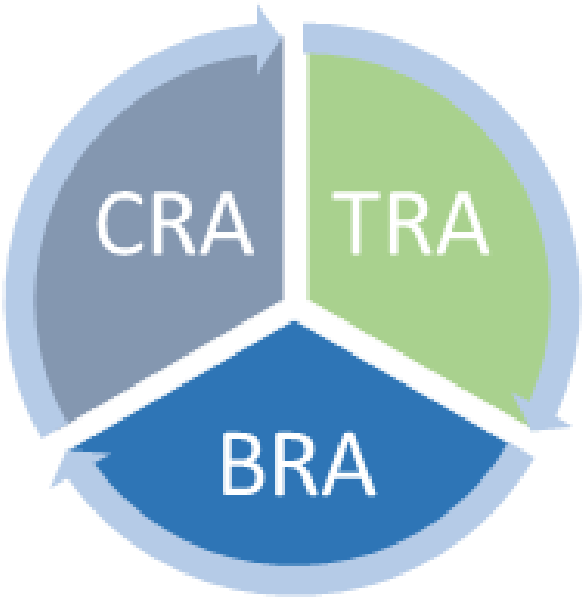
(3) The customer risk assessment must have regard to all relevant risk factors, including —

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

73%
Compliance with paragraph 6(3)(a) of the Code

Paragraph 6(3)(a) of the Code requires that the CRAs must have regard to the outcomes of the firm's BRA. Whilst almost three quarters of the firms were compliant with this paragraph of the Code, the Authority's officers observed that many firms could further enhance the detail of the interplay between the BRA and CRA to better demonstrate compliance with the Code.

The BRA, CRAs and TRA are interconnected, with each type of risk assessment informing the other. With the outcomes and findings from the CRAs informing and influencing both the BRA and TRA, risk assessments and mitigation measures are in a continuous feedback loop. As a prescribed relevant risk factor of the Code with a fairly wide scope, relevant persons should always ensure that they adequately detail the consideration of aspects of the CRA within the BRA and vice versa, identifying and documenting all potential risks posed to the business in relation to this risk factor within their CRA.



In some cases, firms did not document the outcomes of the CRA in the BRA and likewise did not reflect the conclusions of the BRA in the CRA or make reference to the BRA in the CRA procedure, therefore failing to identify and document the ML/FT risks and vulnerabilities associated with their unique business, customers, products and services.

It should be noted that including a small or non-specific mention of a firm's BRA in its CRA procedure is also not sufficient to demonstrate effective compliance with the Code, there should be clear reference to how the outcomes of one have affected the other.

Handbook quote

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.

Paragraph 6(3)(a) - Best Practice:

The CRA should ensure consideration of the findings and outcome of BRA:

1. The findings of the BRA, including the NRA should inform each CRA and the underlying methodology.
2. 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.
3. Use the results of the BRA to inform the question set of the CRA along with the risk scores and weightings.

Paragraph 6(3)(b) of the Code

6 Customer risk assessment

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

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

83%
Compliance with paragraph 6(3)(b) of the Code

Paragraph 6(3)(b) of the Code requires for the CRA to have regard to the nature, scale, complexity, and location of the customer's activities. The Authority's officers noted that the vast majority of firms were compliant with this paragraph of the Code and further noted a wide array of methods for considering these factors in the CRA, a large number of which were tailored to and appropriately recorded the specifics of the customer.

When identifying and assessing the ML/FT risks associated with the nature, scale, complexity and location of the customer, consideration should include the following aspects of the customer's profile. The Handbook provides further guidance on effective compliance with paragraph 6(3)(b) of the Code in section 2.2.9.2.

When considering the **NATURE** of the customer, it is important to collect information on:

- The nature of the customer relationship, or the customer's activities; or
- Political connections, other prominent positions or high public profile; or
- Links to sectors that are commonly associated with, higher risk of bribery, corruption, ML/FT/PF or significant amounts of cash. – Examples of such sectors are:

- 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.

- Virtual asset service providers.

Items of consideration when assessing the **SCALE** of the customer's activities, relevant persons should consider:

- The anticipated (and realised) turnover of the customer's business; or
- The value, net-worth, volume of activity and value of activity associated with the customer; or
- The location of the customer's operations, particularly if more than one jurisdiction is involved; or
- The occupation or activity of the customer.

When considering the **COMPLEXITY** of the customer, information or areas to consider include:

- If the customer is an individual or a legal entity; or
- The customer's former, current, or planned business activity; or
- That activity being complex trade deals, third party involvement, dealing with a complex and technical sector that the customer may lack the expertise in; or
- The customer's SOF and/or SOW.

The considerations of risks presented by the **LOCATION** of the customer's activities should include, at a minimum:

- The location of the customer's operations;
- The address of the customer, if different from the above; or
- The location(s) associated with the SOF and/or SOW; or
- Any connection with countries on List A or List B.

An example of good practice noted by the Authority's officers in several cases, was the addition of a written summary or conclusion of the customer within the CRA, to further justify and explain the applied risk rating.

The summary, in all cases, detailed information that the CRA may not have specifically requested but that the relevant person factored into the final risk rating, either as a risk factor or as a mitigation of a risk factor. In particular, the written summary was helpful when evidencing a full and intricate understanding of the customer and the associated risks. Documenting rationale as part of the CRA is a positive step in taking risk assessments beyond a 'tick box' exercise.

The addition of a written summary or conclusion of the customer within the CRA helps to further explain the risk rating

Paragraph 6(3)(b) - Best Practice:

- The CRA builds a clear picture of the customer's activities, allowing for effective risk assessment.
- The queries are tailored to the specifics of the customer.
- Where a legal entity is the customer, consideration is also given to the profile of the beneficial owner.
- Consideration is made of the structure of the customer.
- Consideration is made for the value of the customer.
- Consideration is made of the customer's proposed business activity; and
- Such consideration is compared against the actual activity when the CRA is reviewed.
- There is a summary of the Nature, Scale, Complexity, and location of the customer's activities.
- Demonstrates an understanding of the customer and evaluation of the risks.

Case Study 2:

The Authority's officers observed a strong example of compliance with this paragraph of the Code whereby the CRA was structured in a sectioned, structured format with additional commentary provided at the end of each section. The CRA contained two sections titled 'Nature, Scale and Complexity of the entity' and 'Geographic and country risk' which included standardised questions that had been tailored to the expected customer base of the relevant person. These questions were complimented with observations on the specifics of the customer in the comments field of both sections. The CRA at the outset queried the type of customer entity (such as individual, trust, company, or partnership), the purpose of the business and the purpose of the relationship with the relevant person.

These initial queries shaped the subsequent CRA with some key items including risk assessments of the jurisdictions of any shareholders/other controlling parties of the customer, the location of the client base of the customer, the location of the operations of the customer and the suppliers of the customer (where such risk factors were applicable). Each query was given a risk score, and the summation of these risk scores was distilled into a final risk rating using a clearly defined methodology.

Paragraph 6(3)(c) of the Code

6 Customer risk assessment

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

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

80%
Compliance with paragraph 6(3)(c) of the Code

Handbook quote

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.*

The Authority's officers noted that, for the most part, the CRA procedures and controls that the Authority's officers reviewed accounted for the manner in which products and services are provided to the customer. This was, in most cases, reviewed by the Authority's officers, tailored to the range of products provided by the relevant person and the manner in which they usually contact their customers. Where relevant persons have contravened this paragraph of the Code, this was as a result of not having any regard to this risk factor or providing very little narrative around it.

In accordance with the Handbook, when identifying and assessing the ML/FT risks associated with the provision of a relevant person's products, services and transactions, consideration should be given to the risks related to:

- 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.

Section 2.2.9.2 of the Handbook provides further detail around the potential ML/FT risks associated with certain products, services, and transactions.

Consider how technology is used in delivering products and services

Paragraph 6(3)(c) - Best Practice:

- Detailed narrative is recorded around how the various products and services are provided by the relevant person.
- Regard is given to the outcomes of the BRA when considering the risk of a product or service.
- Consideration of the ML/FT risks associated with the relevant person's interactions with their customers.
- Regard is given to whether introducers or intermediaries are used and the nature of such use.
- Consideration of the way technology is used in delivering products and services.

Paragraph 6(3)(d) of the Code

6 Customer risk assessment

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

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

59%
Compliance with paragraph 6(3)(d) of the Code

Paragraph 15(5) of the Code

(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.

Handbook quote

Location of the customer's activities - Geographic risk

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

Paragraph 6(3)(d) of the Code requires the CRA to have regard to the risk factors included in paragraph 15(5) and (7) of the Code.

These paragraphs of the Code contain 'matters that pose a higher risk of ML/FT.' As per the Handbook, the risk factors at paragraph 15(5) of the Code must be treated as higher ML/FT risk and business relationships/occasional transactions where such matters are relevant must be treated as higher risk and subject to ECDD, the Handbook goes on to state that the risk factors listed 15(7) are matters that may pose a higher ML/FT risk.

Whether they in fact pose a higher risk is a matter for relevant persons to determine in the context of their BRA, CRAs and TRA.

Where relevant persons have contravened this paragraph of the Code, this was usually the result of the omission of relevant factors in paragraphs 15(5) and/or 15(7) of the Code when undertaking or reviewing a CRA.

Relevant persons should document and evidence its assessment of and regard to these risk factor, including the following aspects of the customer and the relationship:

- whether a customer is resident in, located in or, has activity in a jurisdiction in List A or List B.
- whether a customer is the subject of a warning in relation to AML/CFT matters issued by a competent authority.
- PEP involvement in the business relationship.
- nominee or bearer share arrangements.
- whether the customer themselves may be a high net worth individual.
- circumstances wherein the customer is not met face to face at any point during the business relationship.

Paragraph 15(7) of the Code

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

(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.

Paragraph 6(3)(d) - Best Practice:

- High risk factors are explicitly denoted in the CRA.
- Regard is given to the relevant person's risk appetite when considering the factors in paragraph 6(3)(d) of the Code.
- High risk factors trigger a higher risk rating and are mitigated against.
- High risk factors require additional sign-off at the onboarding stage.
- High risk factors warrant more frequent review of the customer and the CRA.
- Consideration is given to additional CDD that may be required when high risk factors are identified.

Case Study 3:

A strong example of compliance observed by the Authority's officers in relation to paragraph 6(3)(d) of the Code included the CRA having a separate "High Risk Factors" section which recorded, and risk rated the factors outlined above, with a further 'Higher Risk of ML/FT' section, which listed additional factors, specific to the relevant person's risk appetite, that should be considered when undertaking the CRA.

The CRA clearly identified high risk factors using the Code, the Handbook sector specific guidance, the specifics of the relevant person's risk appetite. The firm utilised those factors to identify existing relationships that exhibited one or more of those factors as business relationships that may carry an increased risk of ML/FT/FC and/or PF.

The benefit of this process allowed for a clear narrative to be established around the relevant persons understanding, controls and mitigations of such risks and thereby evidencing strong compliance with the Code.

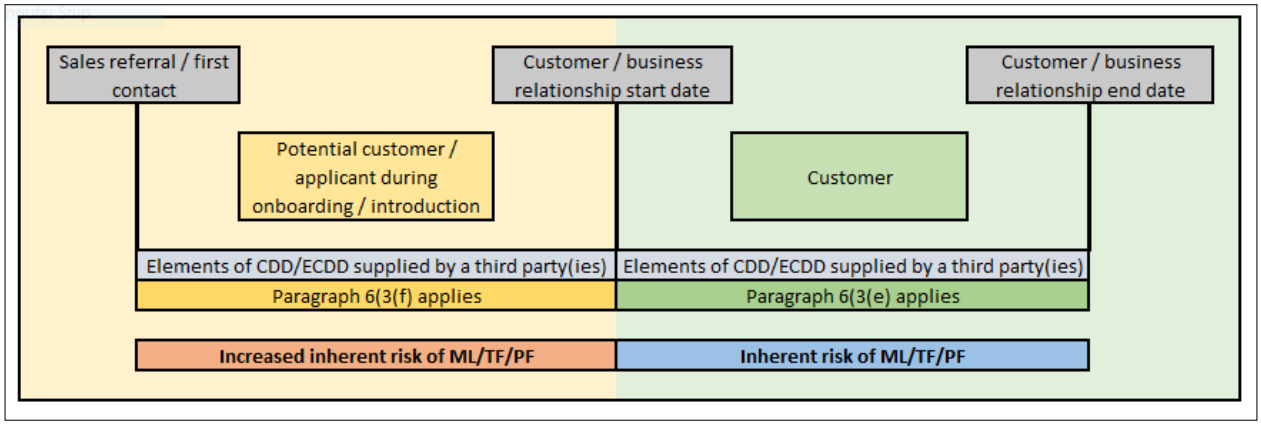
Paragraph 6(3)(e) of the Code

6 Customer risk assessment

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

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

75%
Compliance with paragraph 6(3)(e) of the Code



Handbook quote

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.

Paragraph 6(3)(e) of the Code details that the CRA must have regard to the involvement of any third parties for elements of the CDD process[5], including where reliance is placed on a third party. Third party involvement can occur in a number of ways, to various degrees and at various times during the business relationship.

For clarity, this risk factor covers any scenario from the provision of elements of CDD by a party who is not the customer after the on-boarding of that customer to the continued provision of CDD through any third-party connection who has a relationship with the firm.

Involvement of a third party in the business relationship, at any point, should generally be considered a higher inherent ML/FT/PF risk factor than a strictly direct customer-firm relationship, with such additional risk being appropriately reflected in the CRA.

When identifying and assessing the ML/FT risks associated with outsourcing elements of the CDD process, consideration should include:

- the quality of control mechanisms in place with the provider, such as clarity of the division of roles and responsibilities and the quality of management information and reporting.
- whether the third party is a trusted person[6].
- 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.

[5] "Elements of the CDD process" is detailed further in section 3.4.3 of the Handbook.

[6] As defined in the Code

Paragraph 6(3)(e) - Best Practice:

- Detailed narrative is recorded around how the relevant person has collected the required CDD and/or ECDD.
- Regard is given to the risks associated with any third party, or chain of third parties, involved in the process.
- Reliance agreements with third parties are clearly recorded and tested in line with internal compliance testing procedure.
- Addition or removal of a third party in the CDD process is reflected in the initial and ongoing review of CRAs.

Paragraph 6(3)(f) of the Code

6 Customer risk assessment

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

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

76%
Compliance with paragraph 6(3)(f) of the Code

Handbook quote

Customer risk assessments carried out under paragraph 6 of the Code.

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.

Paragraph 6(3)(f) of the Code requires firms to document any assessment of an introducer in circumstances where a customer has been introduced. In cases where business is introduced, the Authority's officers would expect to see a comprehensive risk assessment of the introducing firm or introducer.

The objective of assessing the introducing firm is to ensure that the relevant person is aware of the potential ML/FT risk of introduced business and that such risks are accurately reflected in the CRA, ensuring appropriate scrutiny and mitigation is applied to introduced business relationships applying a risk-based approach.

For example, this should include risks associated with the geography and reputation of the third party or the previous interactions with the same. Including assessment of the usual types/profiles/patterns of customers the introducer has previously introduced to the relevant person, where applicable. Additional guidance on the introducer risk assessment, specified considerations pertaining to third parties and how these integrate with the CRA can be found in section 2.2.10 of the Handbook.

Case Study 4:

One example, seen by the Authority's officers, demonstrated effective compliance with paragraph 6(3)(f) of the Code by including a full, separate risk assessment for the introducer of the customer. The introducer risk assessment shared a number of factors with the CRA, including the location of operations, the risk of the operations of the introducer and the risk of factors such as adverse media, PEP and sanctions exposure. The introducer risk assessment went on to detail and assess the processes that the introducer goes through when introducing customers, whether the customer and introducer have met face to face, whether any elements of CDD provided by the introducer have been obtained directly or from an additional third party. Concluding thereafter with an evaluation of the risk of the introducer, which was then considered in the original CRA. It was subsequently evidenced to the Authority's officers that the introducer risk assessment was reviewed in tandem with the CRA, ensuring a consistent and well documented assessment of the facets of the customers risk profile.

Paragraph 6(3)(f) - Best Practice:

- Provides a detailed breakdown of the introducer's risk profile.
- Considers how the risk profile of the introducer affects the risk of the customer.
- Considers how the specifics of a given introduction influence the risk of the customer.
- Regularly reviewed in order to ensure the most up to date information possible is assessed; and
- The outcomes of such review are considered thereafter in the ongoing CRA.

Paragraph 6(3)(g) of the Code

6 Customer risk assessment

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

(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

84%
Compliance with paragraph 6(3)(g) of the Code

Handbook quote

Whether the relevant person and the customer have met during the business relationship, or its formation.

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.

Paragraph 6(3)(g) of the Code requires the CRA to have regard to whether the relevant person and the customer have met during the business relationship, or its formation. Firms should ensure that they document and evidence their procedures and controls 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, in order to best demonstrate compliance with the Code.

The Authority's officers observed a range of different ways firms complied with this paragraph of the Code, with some firms not accepting any non-face to face interaction with customers, and others carrying "out real-time visual communication media online over the internet such as full-motion video conferencing"[7] and documenting such meetings including screenshots of the customer holding identification documents and address proof documents, which are then certified an appropriate member of staff present in the meeting.

Case Study 5:

In one case, seen by the Authority's officers, whilst the policy allowed for an initial online meeting to be considered face to face, this was re-enforced by a requirement of the same policy to physically meet the customer as soon as reasonably practicable after the establishment of the business relationship.

The CRA reflected this by considering an online meeting as acceptable, but with a slightly higher risk rating than a physical meeting. Following the face-to-face meeting with the customer this risk was considered mitigated and a review of the CRA was undertaken.

As such, the risks were clearly documented and understood, with the CRA and CRA review providing a narrative around the risks identified and mitigations applied, thereby evidencing strong compliance with the Code.

[7] Anti-Money Laundering and Countering the Financing of Terrorism Supplemental Information Document July 2021

3.5 Summary/Conclusion

The observations, findings, recommendations and best practices identified within this report should be considered, and where relevant, implemented by all relevant persons in their compliance with the Code. The Authority reiterates that compliance with the Code is mandatory, and all relevant persons should use the range of resources available to assist in complying with the requirements of the Code, including; the Handbook, sector specific guidance, webinars, reports, and public statements the Authority issues and publishes.

Legislation and Guidance	Web Links
The Anti-Money Laundering and Countering The Financing of Terrorism Code 2019	**Link**
The Anti-Money Laundering and Countering The Financing of Terrorism Handbook December 2023	**Link**
Supplemental Information Document July 2021	**Link**
The Isle of Man Financial Services Authority AML/CFT Regquirements and Guidance webpage	**Link**
The Isle of Man Financial Services Authority TCSP Thematic Report Phase 1	**Link**
The Isle of Man Financial Services Authority Webinars webpage	**Link**

ISLE OF MAN
FINANCIAL SERVICES AUTHORITY

Lught-Reill Shirveishyn Argidoil Ellan Vannin

Our mailing address is: PO Box 58 Douglas Isle of Man IM99 1DT

Email: aml@iomfsa.im