ISLE OF MAN
FINANCIAL SERVICES AUTHORITY

Lught-Reill Shirveishyn Argidoil Ellan Vannin

MAY 2023

FOREIGN PEP THEMATIC REPORT

www.iomfsa.im

aml@iomfsa.im

Contents

Colour key used in this document: AML/CFT Code 2019 | AML/CFT Handbook | General information

1. Foreword by the CEO

The Isle of Man Financial Services Authority ("the Authority") is responsible for oversight of anti-money laundering and countering the financing of terrorism ("AML/CFT") compliance for those involved in the financial sector and a range of other designated businesses, together with oversight of compliance with the Beneficial Ownership Act 2017.

The Authority's work is driven by its three main regulatory objectives:

>>> Protecting consumers;

>>> Reducing financial crime; and

>>> Maintaining confidence in the financial services sector through effective regulation.

A key part of delivering on our regulatory objectives is through effective supervision and oversight of regulated firms and designated businesses (together, "firms" or "relevant entities"). The Authority operates an approach whereby it focuses its finite resources on firms and activities that pose the greatest potential impact and/or risk to its objectives.

When it comes to AML/CFT, a key element of the Authority's role is to test and challenge firms' compliance with the Isle of Man AML/CFT Framework. Firms have legal obligations to help prevent illicit money in their business and the Island. Compliance weaknesses and failures found here do not require there to be direct evidence of money laundering or terrorist financing.

The Authority recently undertook a thematic exercise that involved reviewing processes and procedures used by firms in managing Politically Exposed Persons ("PEPs"). This report explains the scope of that exercise, outlining the steps that were taken and the numbers of firms that were reviewed, and highlights some of the key findings.

While the reviews noted evidence of good practice, overall a significant number of contraventions were identified across firms*. Considering the higher risk presented by PEPs, it is essential for firms that take on these customers to have robust controls in place, as well as staff with the right skills to deal with this type of customer. The Authority is continuing to work with firms regarding next steps, either in respect of remediation plans or to refer matters to our Enforcement Division for consideration as appropriate.

We hope this report will be helpful in providing some learning points and suggestions of good practice to all firms, whether they were involved in this particular thematic or not. This report should be considered alongside the content of the Authority's AML/CFT Handbook, which should be used as a resource when developing appropriate procedures and controls. The Authority will not be publishing inspection reports or detailed findings from each inspection in this document. An inspection report has been provided to each firm inspected.

Bettina Roth, Chief Executive Officer

Isle of Man Financial Services Authority

> *We hope this report will be helpful in providing some learning points and suggestions of good practice*

*** The contraventions referred to in this report are those identified by the Authority within the inspection reports.**

2. Introduction

As a small jurisdiction with a wide and ambitious reach, the Isle of Man ("IoM") has corresponding obligations to protect itself and others from financial crime, in particular cross-border international crime such as the laundering of the proceeds of corruption.

The Island's approach in relation to preventing ML/FT and financial crime is set out in the IoM Government's Financial Crime Strategy. The Strategy confirms the Island's commitment "to meet international standards including those relating to money laundering and terrorist financing."

The ability of the IoM to continue to attract, and retain, legitimate customers with clean funds depends in part on the reputation of the Island as a sound and well-regulated jurisdiction. The effectiveness of this protection, and the reputation of the Island, depends on the vigilance of relevant entities.

The IoM National Risk Assessment 2020 ("NRA") identified bribery and corruption as one of the main crimes presenting an international threat to the Island. This accounts for approximately 17% of current matters with the Economic Crime Unit. This threat arises substantially from those seeking to launder proceeds of these offences through the IoM, rather than from domestic predicate offences.

The NRA highlights that bribery and corruption may involve PEPs directly or indirectly through introducers, intermediaries or complex structures.

Purpose of review

The purpose of the Authority's foreign PEP thematic exercise was to consider one of the key international crime threats to the Island's reputation, and to test the strength of firms' preventative measures and controls against this threat.

3. AML/CFT Code obligations

As part of the commitment to protect the Island from ML/FT, the Anti-Money Laundering and Countering the Finance of Terrorism Code 2019 ("AML/CFT Code" or "the Code"), sets out the legal obligations for businesses in relation to the prevention of ML/FT. These obligations include the keeping of records and evidence, identifying and verifying the identities of customers, and operating an appropriate and effective risk-based compliance regime.

The importance of maintaining an understanding of the overall ML/FT risks faced by the business cannot be overstated. This understanding and the application of appropriate procedures and controls can assist a firm in satisfying itself that it is not handling the proceeds of crime, therefore mitigating the risk of ML/FT. Not giving this area adequate attention on an ongoing basis exposes the firm, and the Island, to the increased risk of facilitating financial crime.

The Code is designed to ensure that relevant entities identify what ML/FT risks they may face, and can demonstrate they are taking reasonable steps to mitigate the negative effects. The IoM must be able to evidence that relevant entities are fulfilling their Code obligations in order to demonstrate that the Island's regulatory framework meets international standards to protect against ML/FT.

As mandated by the Code, relevant entities must:

>>> produce Customer Risk Assessments ("CRAs") which document and explain the risks presented by individual customers;

>>> develop a Business Risk Assessment ("BRA") which covers the firms' activities, the risks they face, and their risk appetite. A BRA must have regard to CRAs, customer group risk, and the Technology Risk Assessment ("TRA") in forming the firm's overall risk assessment of the business; and

>>> apply effective customer due diligence ("CDD" or enhanced "ECDD") checks and controls throughout the customer life cycle.

Due to the additional risks that PEPs can pose, additional measures and controls are required if prospective or existing customers are, or become, PEPs. Relevant entities are required to retain as a record documentary evidence of any further consideration of risk, PEP checks, additional measures applied, and how the ML/FT risks have been suitably mitigated.

These Code requirements include:

>>> documenting senior management approval prior to the acceptance or continuation of the provision of services;

>>> conducting additional CDD/ECDD checks[1]; and

>>> undertaking an enhanced level of ongoing monitoring, alongside the review and update of CRAs at regular or trigger event-driven intervals.

The Authority's AML/CFT Handbook ("the Handbook") provides information and guidance to help relevant entities consider their obligations. Section 2.2 offers guidance on carrying out the risk assessments required under the Code, and explains the fundamentals of a risk-based approach.

"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 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."

[1] The additional measures apply automatically to Foreign PEPs no matter the risk of ML/FT posed, however enhanced requirements do not automatically apply for domestic PEPs unless there are other higher risk factors.

4. Executive Summary

In order to evaluate the scope of the risks faced by relevant entities in the IoM, and test the mitigation controls that are in place, the Authority undertook a thematic exercise between 2021 and 2023 to assess the AML/CFT preventative measures and controls that firms apply in respect of foreign PEPs.

The outcomes from the thematic exercise inform the Authority's own picture of risk in relation to foreign PEPs and will also inform the Island's NRA.

The thematic exercise consisted of two core phases. Data collection and analysis comprised Phase 1, followed by thematic inspections in Phase 2. The objectives of the thematic inspections are included in section 7.1 of this report.

This overarching report, covering both stages of the thematic, reflects the findings from a broad spectrum of firms of varying sizes operating across different sectors. The report will provide insight to firms that are regulated or supervised by the Authority as to whether their own controls are relevant to their business, and are, most importantly, effective.

We would like to thank the firms involved for their time and effort in dealing with information requirements, and for handling comments and queries from the Authority's officers.

Firms with connections to foreign PEPs were identified from AML/CFT returns submitted to the Authority. Further details were obtained from a cross-section of those firms (91 firms) via a bespoke questionnaire. Following analysis of this data, focused risk-based inspections were then carried out on 29 firms.

> *The report will provide insight into whether firms' own controls are relevant and effective*

The firms included within Phase 1 of the thematic exercise were split as follows:

- **8** Banks
- **25** Insurance and pensions providers
- **33** Trust and Corporate Services Providers
- **12** Fund Managers and Investment firms
- **13** Designated Businesses

Almost all of the firms inspected have further work to do in order to meet the requirements of the Code, and to be able to demonstrate an effective compliance regime which successfully attempts to prevent ML/FT. In some cases the necessary remedial action is relatively small in scale and can be completed quickly by the firm. In other instances, the gaps and weaknesses that have been identified mean that significant remedial action will be required in order to correct past failings and to ensure that firms have robust policies, procedures and processes going forward.

In a number of cases where the identified contraventions were both material and significant, the case has been or will be considered (as applicable) by the Authority's Enforcement Division, in addition to remedial actions being undertaken.

5. Summary of Phase 1 data
(across 91 firms)

A specific questionnaire was issued to 96 firms, and completed by 91 (5 being nil returns[2]). The data received in 2021 from the questionnaire included:

>>> the number of foreign PEPs within the customer base;

>>> the PEP's nationality/country of residence;

>>> the category/role of the foreign PEPs[3];

>>> details of the type of controls and approaches taken by the firm with regard to PEPs such as –

- details of screening tools utilised;
- maintenance of PEP registers; and
- any reporting to law enforcement authorities.

Across the 91 firms, there were more than 10,000 unique foreign PEPs[4]. Almost 95% of foreign PEP numbers came from the Life Insurance (62%), Banking (17.8%), and Fiduciary Services (14.5%) sectors. The largest contingent of foreign PEPs are UK nationals (31%), whereas 27% of the foreign PEPs are resident in the UK. The data suggested 64% of PEPs reported still held a PEP position/were associated with a PEP still in post.

Some key findings from the data collected as part of Phase 1 are as follows:

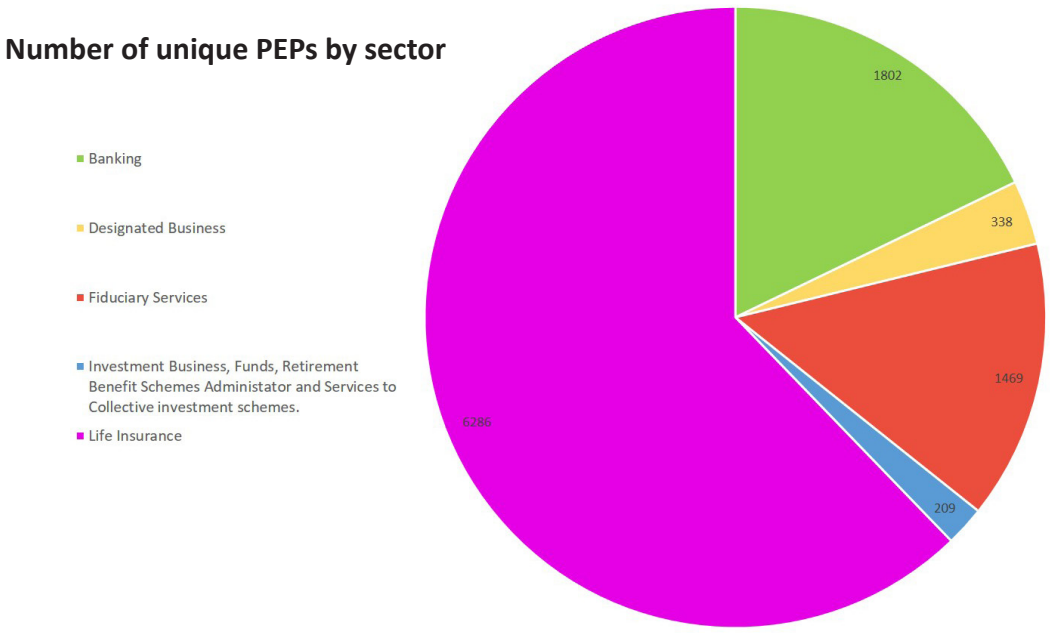
>>> 100% of firms maintained a register of PEPs;

>>> 80% used an automated screening system to assist in the identification of PEPs (usually in conjunction with manual screening);

>>> more than 60% of firms asked prospective customers at the outset of the business relationship if they were a PEP,

>>> the number of prospective PEP customers who had been declined on the basis of ML/FT risk was low; and

>>> the number of external disclosures made was also low.

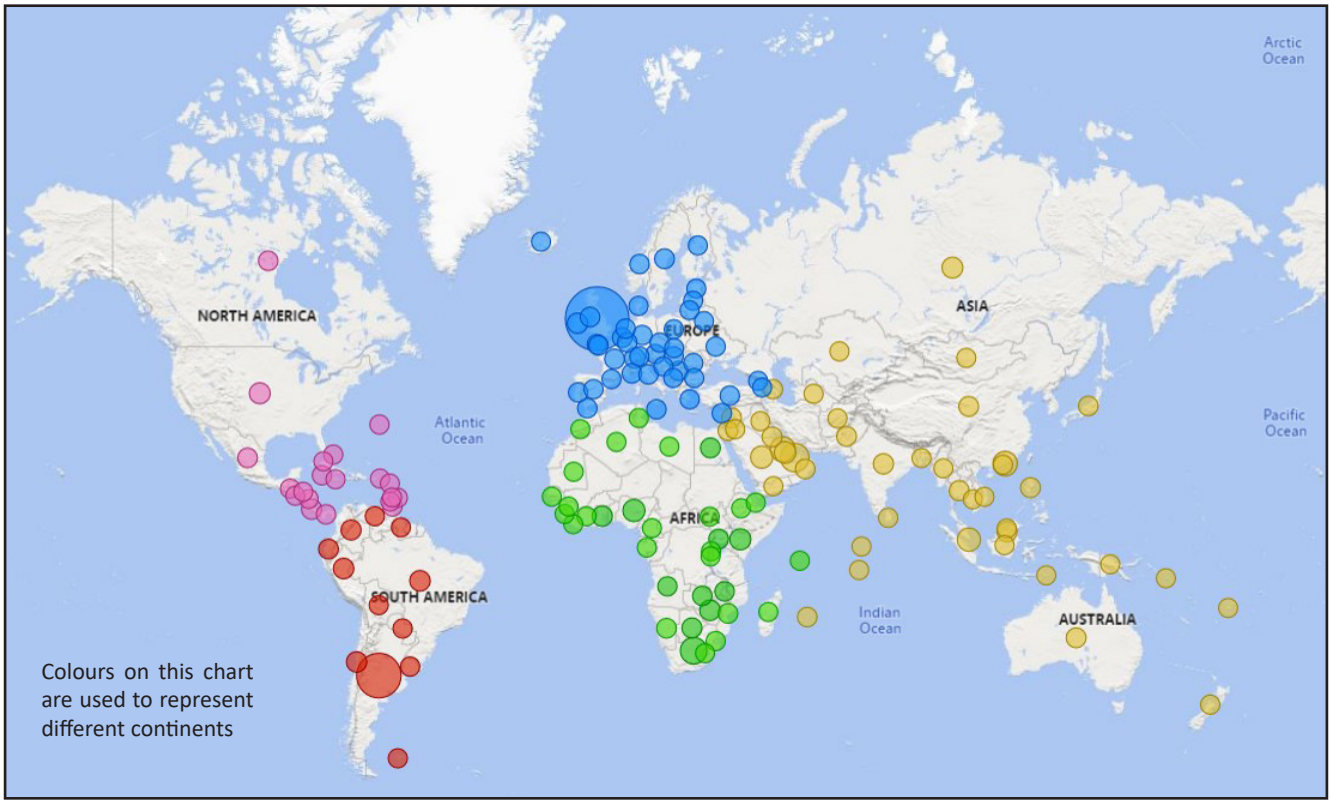


[2] 96 questionnaires were circulated, however five were nil returns, therefore the data is based on findings from 91 firms. These five entities were included in Phase 1 for completeness as they are connected group companies to others that were selected in Phase 1 of the thematic exercise.

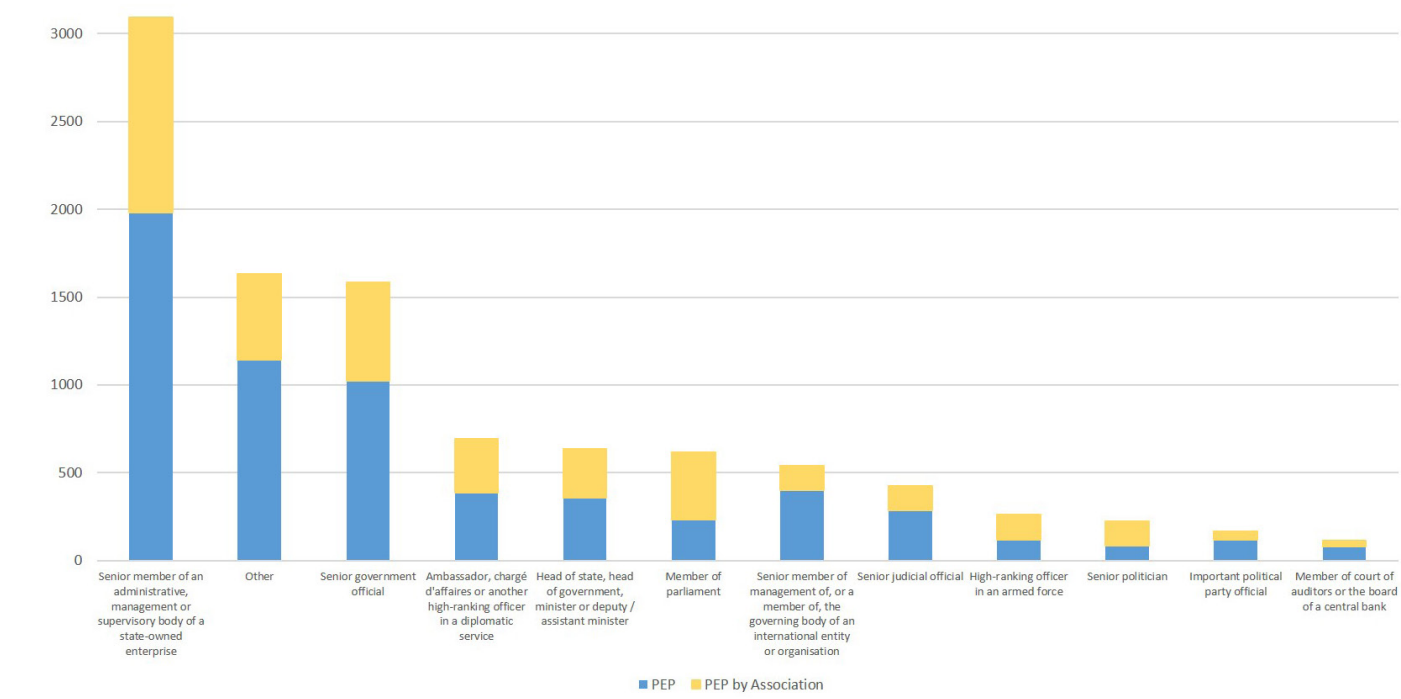
[3] The data gathered did not involve personal or identifying details of individuals.

[4] Individuals determined to be Foreign PEPs

The residency/nationality[5] of unique foreign PEPs reported in Phase 1 data

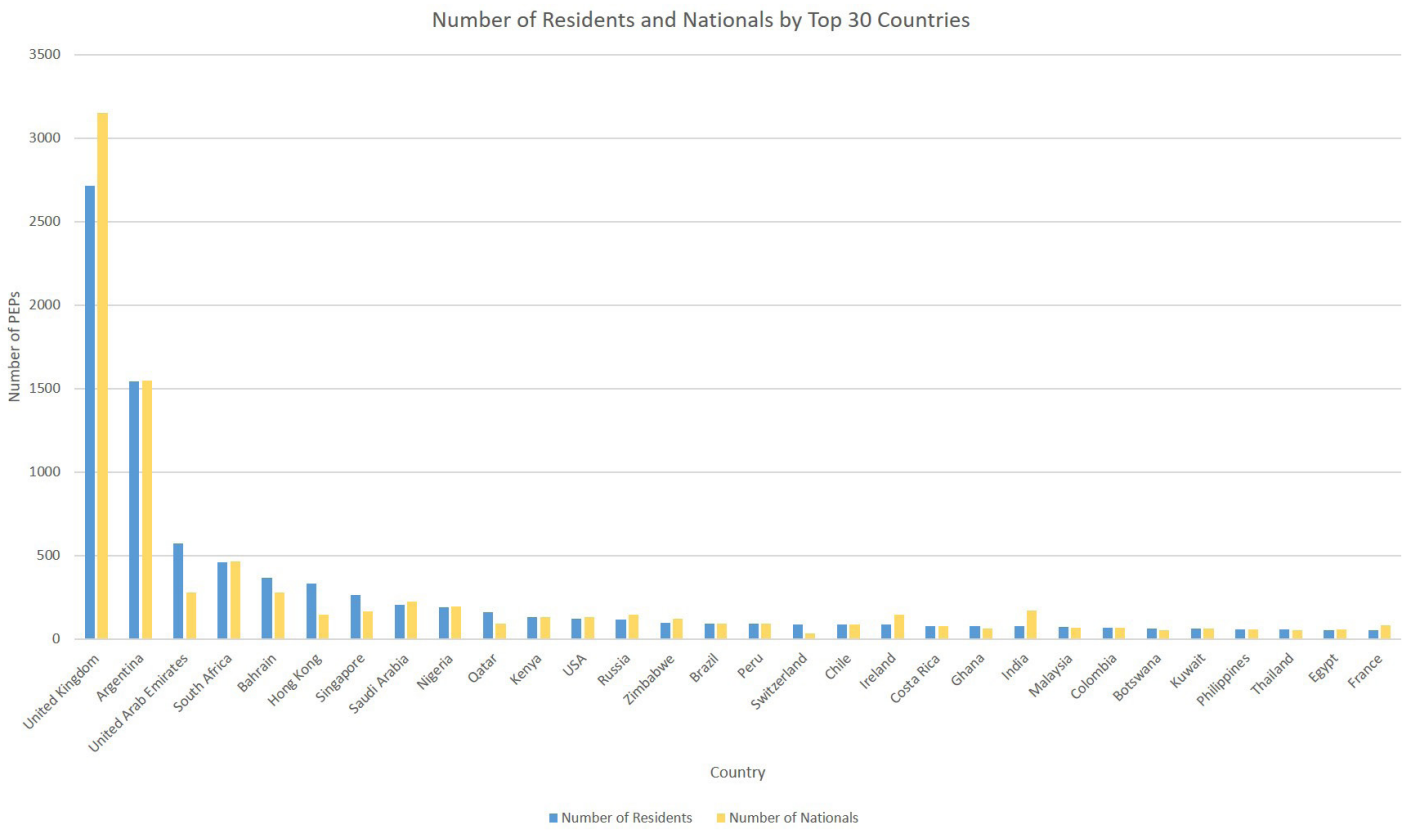


Roles held by foreign PEPs and associates reported in Phase 1 data



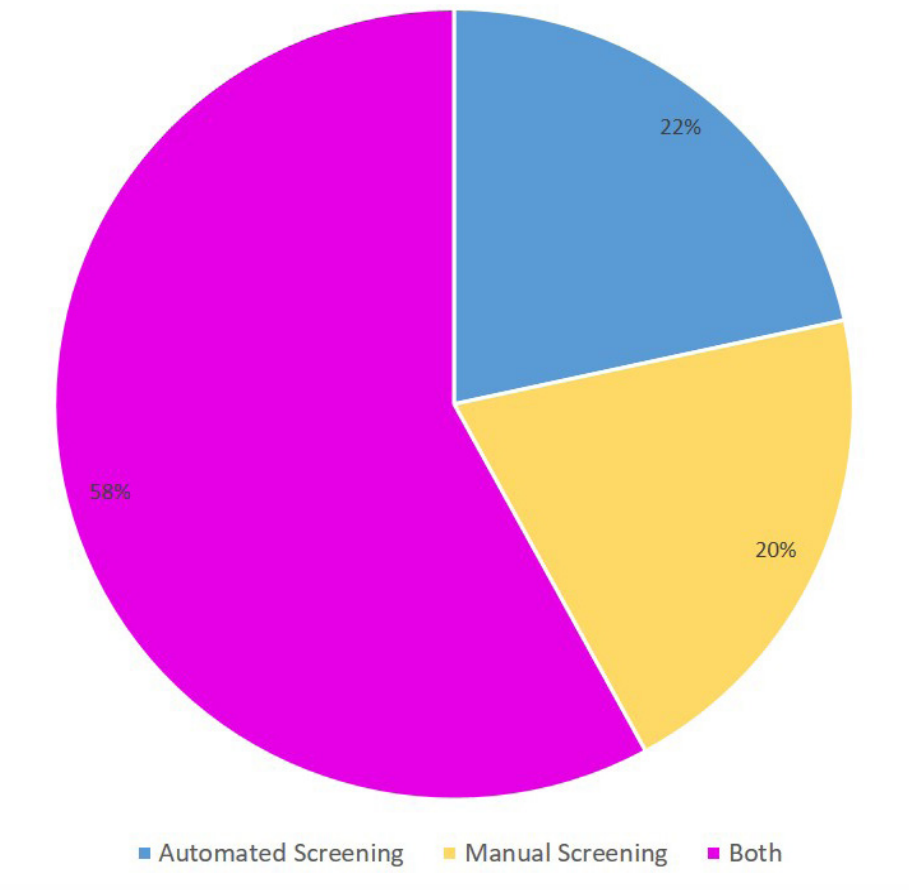
[5] The data relating to residency/nationality of foreign PEPs was almost identical and both result in similar concentrations on a map, therefore this map can be used to represent both residency and nationality of foreign PEPs.

Foreign PEPs by top 30 countries - number who are residents and number who are nationals



Foreign PEPs by top 30 countries - number who are residents and number who are nationals

Screening methods used to identify PEPs



6. Phase 2 findings:
(across 29 firms)

Across the firms that were subject to inspection as part of the second phase of the thematic exercise, a range of approaches to Code compliance were identified. The Authority's officers found that there were differences across firms' understanding of ML/FT and the requirements of the Code, and that firms displayed strengths and weaknesses in a variety of areas.

Minor weaknesses will require only a small amount of remediation, whereas firms that displayed failings of a more material nature will need to invest in new or updated systems, procedures and controls, and achieve a greater level of AML/CFT comprehension amongst their staff. In addition to the need for remediation work, at the time of drafting this report, a number of firms with identified significant, material contraventions have been referred to the Authority's Enforcement Division for further consideration.

It is important to note that many areas of the Code are interconnected, such as risk assessment and control requirements. Therefore, in many cases, weaknesses in some areas had the knock-on effect of causing weaknesses or gaps in multiple areas of the firm. This resulted in the recording of additional contraventions of the Code. As an example, poor quality or non-existent CRAs can result in an incomplete picture of risk across the business, and makes it less likely that appropriate risk based controls, such as CDD/ECDD and ongoing monitoring, can be established and applied.

Contraventions of the Code were mainly in relation to the following areas:

>>> Paragraph 4: Procedures and controls

>>> Paragraph 5: Business Risk Assessment

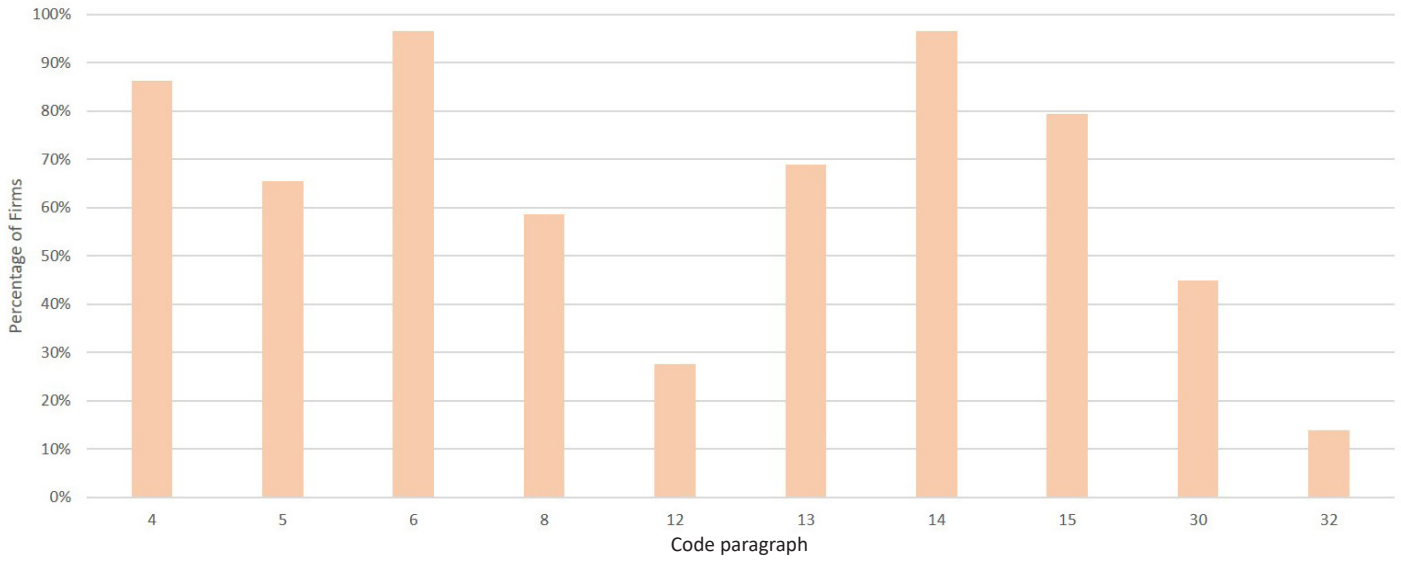
>>> Paragraph 6: Customer Risk Assessments

>>> Paragraph 13: Ongoing monitoring

>>> Paragraph 14: Enhanced measures for PEPs

>>> Paragraph 15: Enhanced Customer Due Diligence

Comparison of Code contraventions[6] across all sectors



[6] This chart includes the main paragraphs contravened, as identified by the Authority's inspection reports,not all Code paragraphs considered on inspections. Paragraphs 9, 10, 11, 19, 22, 33, 34, 35 are omitted from the chart. In addition, it is important to note differing numbers of inspections took place across sectors, with the fiduciary sector having the most inspections during the thematic exercise. Some cases remain under/are pending review and/or referral.

6.1 Areas of good practice

Several firms clearly had a strong understanding of ML/FT risks, which was supplemented by good systems and controls, clear procedures, experienced staff, and documented evidence of the assessment and management of any identified ML/FT risks.

These firms clearly committed time, effort, and resources to their systems and people in the attempt to protect their business from the use or abuse by criminals. Where issues were found in these firms they tended to be of a minor nature, for example isolated failures to apply controls or infrequent evidential gaps; both of which were simple to correct.

6.1.1 Procedures and controls

The best procedures and controls reviewed were those that were clear and easy to follow. Firms with clear controls and processes, and clear role delineation, tended to find it easier to explain the firm's approach to foreign PEPs, evidence compliance with the Code, and deal with Authority queries during the inspection.

A good practice point in relation to procedures and other documentation required by the Code was to have a clear documented version history in order to demonstrate how long that particular document has been in place.

6.1.2 Business risk assessment

The Authority's officers found some strong examples of firms with a good BRA which is signed off by senior management, and is checked robustly and periodically.

Firms with good understanding of ML/FT risk could implement the right procedures and controls to address the level of risk offered by individual PEPs or PEP associates.

One of the best examples - Business Risk Assessment

Pre-inspection, the firm submitted specific PEP sections from a comprehensive BRA which highlighted additional risk consideration for PEPs. The firm's scoring categories included a "special risk" categorisation above high risk:

>>> Special Risk – PEPs connected to special risk jurisdictions, high-profile persons that could potentially attract international publicity, companies registered or active in a special-risk jurisdiction, nationals or residents in a special jurisdiction, persons whose source of income or funds emanate from a special jurisdiction or one with high reputational risk.

>>> High Risk – Included various triggers including – PEPs connected to high-risk jurisdictions, non-regulated external trustees, complex structures, existing clients with deficient KYC, companies registered in a high-risk jurisdiction, persons whose source of income or funds emanate from a high-risk jurisdiction.

>>> The BRA was up to date and provided a breakdown of the risk categorisation proportions across the firm's customer base, and highlighted the number of active foreign PEP relationships. Alongside this, it set out the inherent risks concerned with PEPs, and how factors which may increase or decrease the ML/FT risk were considered. The BRA outlined the key risks the firm faced from its PEP relationships, where the business risks lie, and what controls it used to mitigate those risks.

Good practice in relation to conducting a BRA includes ensuring the document:

>>> clearly sets out the risks the firm faces in relation to foreign PEPs and their activities and explains the basis of the assessment;

>>> is tailored to the business and risks of that particular firm;

>>> is informed by other risk assessments required by the Code as well as the NRA;

>>> provides detail on the customer base highlighting where key risks lie;

>>> has input from subject or product experts from across the business;

>>> is evidenced as reviewed and signed off by the Board at regular intervals;

>>> is shared with staff across the organisation so they can understand the ML/FT risks faced;

>>> has good version controls (and dated versions);

>>> clearly articulates how much, and what level of, risk the firm is prepared to take[7]; and

>>> details what risk the firm is not prepared to take.

6.1.3 Customer risk assessment

The Authority's officers found some strong examples of firms with good controls and procedures, making effective use of systems along with good individual judgement to produce a detailed assessment of individual customer risks, which is checked robustly and periodically. Firms with good delivery here could robustly evidence the level of risk offered by individual PEPs or PEP associates.

When done well, a CRA which results in a robust and holistic view of the business relationship or occasional transaction and of the risks faced subsequently allows the firm to determine what CDD, controls and monitoring will be required.

Identifying what types and level of controls and checks are appropriate for different customer risks is a key part of taking a risk based approach, and should help those who do it well to apply lower level (and potentially lower resource level) checks and controls to lower risk customers, and enhanced or additional checks to enhanced or higher risk customers.

A good CRA and knowledge of the customer base can also help staff involved in monitoring and ongoing checks to understand what specific ML/FT risks the mitigating controls relate to, and whether there may be changes in the customer risk profile found at checkpoints or transactions.

Information and evidence from CDD controls and monitoring checks must feedback to inform the ongoing CRA.

The best examples included:

>>> where the CRA provided a detailed commentary of the customer, clearly articulating and explaining the assigned risk rating; and

>>> where firms used good third party proprietary suppliers to screen prospective (and existing) customers and used the results to feed into periodic reviews as part of the ongoing maintenance of the CRA.

[7] The BRA may contain further information in relation to the risk management framework, including the entity' risk appetite, or this may be contained in separate policy(s) but clearly cross referenced. It is up to the individual business how this is structured.

Basic good practice in relation to conducting a CRA includes:

>>> understanding and considering the risk factors, recording the evidence and consideration of the individual risk factors as well as the overall outcome of the assessment. The assessment providing an appropriate commentary of the customer and business relationship based on what is known about the customer;

>>> where the dealings with the ultimate client involve complex structures, chains of third parties and/or introducers, including this in the CRA. Additional risk assessments such as an introducer risk assessment on each introducer may also be required;

>>> reviewing regularly, keeping up to date, and recording steps taken during the development or maintenance of the CRA;

>>> considering the risk between the individual CRAs, and using the wider customer population risk to inform the BRA;

>>> regularly checking and refreshing the CRA, so an up-to-date and accurate understanding of the risks from the customer is known and can be reflected in any mitigation, CDD or ongoing monitoring;

>>> flagging possible indicators of PEPs for additional review (dual control or "four-eyes" checks). Do not automatically discount just because the potential match is not 100%;

>>> where there is a procedure in place to override a risk rating the CRA has generated, the Authority would expect this to be considered by someone other than the person undertaking the CRA and usually someone of a higher grade; and

>>> procedures documenting the level of seniority to sign off when on-boarding high-risk customers. It could be considered whether a committee would be useful when making the decision to take on higher risk customers.

6.1.4 Identifying PEPs and on-boarding of PEPs

As part of efforts to mitigate the risk of ML/FT by or through its business, relevant entities need to be able to check and confirm who their customer is (even if the customer is represented by an intermediary or facilitator, or is a beneficial owner of the customer company or trust or similar). Firms need to understand what the business/customer relationship is proposed to be, how the customer proposes to pay/invest, and where the funds come from.

Firms who do this well can be more confident that they know who they are dealing with and, if they have good evidence to demonstrate the ML/FT risk, can make a reasoned decision to on-board a customer and agree the controls needed to monitor this business relationship. This does not prevent the on-boarding of customers who have some higher risks, but the additional checks and tighter monitoring required for higher risks must be capable of protecting the business in preventing ML/FT.

Most firms inspected had appropriate identity and verification documentation for each foreign PEP customer, though some had occasional gaps in customer files when tested. The good examples identified were where firms had thoroughly tested that the customer's source of wealth came from legitimate sources, and also had inbuilt additional controls, monitoring, and management assurance to maintain knowledge and CDD on the customer.

Basic good practice in relation to on-boarding of a PEP includes:

>>> collating evidential documents and corroboration that confirms the customer is who they say they are, with translations where appropriate;

>>> collection of relevant documents and information required by the firm's procedures[8];

>>> determining the CDD or ECDD based on the ML/FT risk posed by the PEP customer; and

>>> taking (and evidencing) reasonable measures to establish SOF/SOW based on the ML/FT risks presented by the customer.

[8] It is possible to deviate from the firm's procedures, however it should be clearly documented why this deviation has occurred and how the ML/FT risks continue to be mitigated.

The Handbook provides information and guidance to help relevant entities consider their obligations in relation to SOF and SOW. Section 3.8 offers guidance on the differences between SOF and SOW and sets out some of the steps that can be taken in order to demonstrate the firm has taken reasonable measures to establish both SOF and SOW.

"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 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 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 only (though relevant persons may of course seek to establish source of wealth for other customers should they determine it appropriate) and it is mandatory for foreign PEP customers. 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. 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."

6.1.5 Ongoing monitoring of PEPs

To ensure that ML/FT risks continue to be mitigated, firms need to check that ongoing transactions and business activity is consistent with the firm's understanding of the customer and business relationship, and that all of this CDD information remains up to date and correct.

Good transaction monitoring tended to be found in firms with high numbers of customers and transaction volumes, matched with good quality monitoring systems and controls applied by staff with a good understanding of the risks involved.

Good practice examples here demonstrated:

>>> that the firm was aware of the higher risks (or possibility of higher risk) from individual foreign PEP customers;

>>> firms had a good combination of screening systems, manual reviews and customer risk assessment procedures; and

>>> evidence of good quality monitoring of adverse and live media, and robust consideration of this triggering refreshed risking of the customer or associate.

6.2 Areas of weakness

Those firms with overly complicated or opaque processes and controls tended to find it more difficult to evidence Code compliance, and therefore required more effort to clarify queries during the inspection. This also tended to apply to firms who did not appear to consider the guidance set out in the Authority's Handbook.

The Handbook sets out the Authority's expectation of the Code requirements and how compliance can be achieved. It is recommended that firms refer to the Handbook when formulating compliance procedures, and have a clear explanation of how their approach still meets Code obligations if they do not follow the guidance.

Within several firms that had weak controls, procedures, and/or risk assessment frameworks (including the BRA and/or CRA), it was noted that frontline staff on the ground deviated from the firm's documented procedures and applied appropriate consideration and controls of their own accord. Although this helped mitigate risks, the lack of appropriate documented controls raised concerns over governance within the firm. Any implemented procedures and controls must be signed off by senior management and the Board, and they should be the driving force to emphasise the importance of risk-based procedures and controls down through the organisation.

Where there are weaknesses in a company's AML/CFT framework, the company could be vulnerable to ML/FT and exposed to a risk that unusual or suspicious activity (as defined in the Code) may not be identified in a timely manner, or not identified at all.

6.2.1 Procedures and controls

A lack of, or failure to apply, effective procedures and controls to protect the firm from the risk of use for ML/FT or abuse by criminals.

Inspection findings included:

>>> gaps in procedure which left staff and the firm exposed to ML/FT;

>>> failures to adhere to the procedures and controls the firm had introduced in order to mitigate identified ML/FT risk. In some cases this was due to a lack of staff awareness of the procedures, and/or lack of awareness of ML/FT risk more generally; and

>>> cases where firms had no, or inadequate, policies, procedures or controls for managing higher risk PEPs. This included one firm whose risk appetite was not to have high-risk PEPs, but had on-boarded customers in this category all the same.

> *It is recommended that firms refer to the Handbook when formulating compliance procedures*

6.2.2 Business risk assessment

A lack of a BRA which is fit for purpose. Inspection findings included:

>>> a firm which had no BRA. In this case the firm was managed or administered by another regulated entity to whom they outsource their AML/CFT. Although the outsourced provider produced a CRA of the firm (as their customer), no BRA had been carried out for the inspected firm;

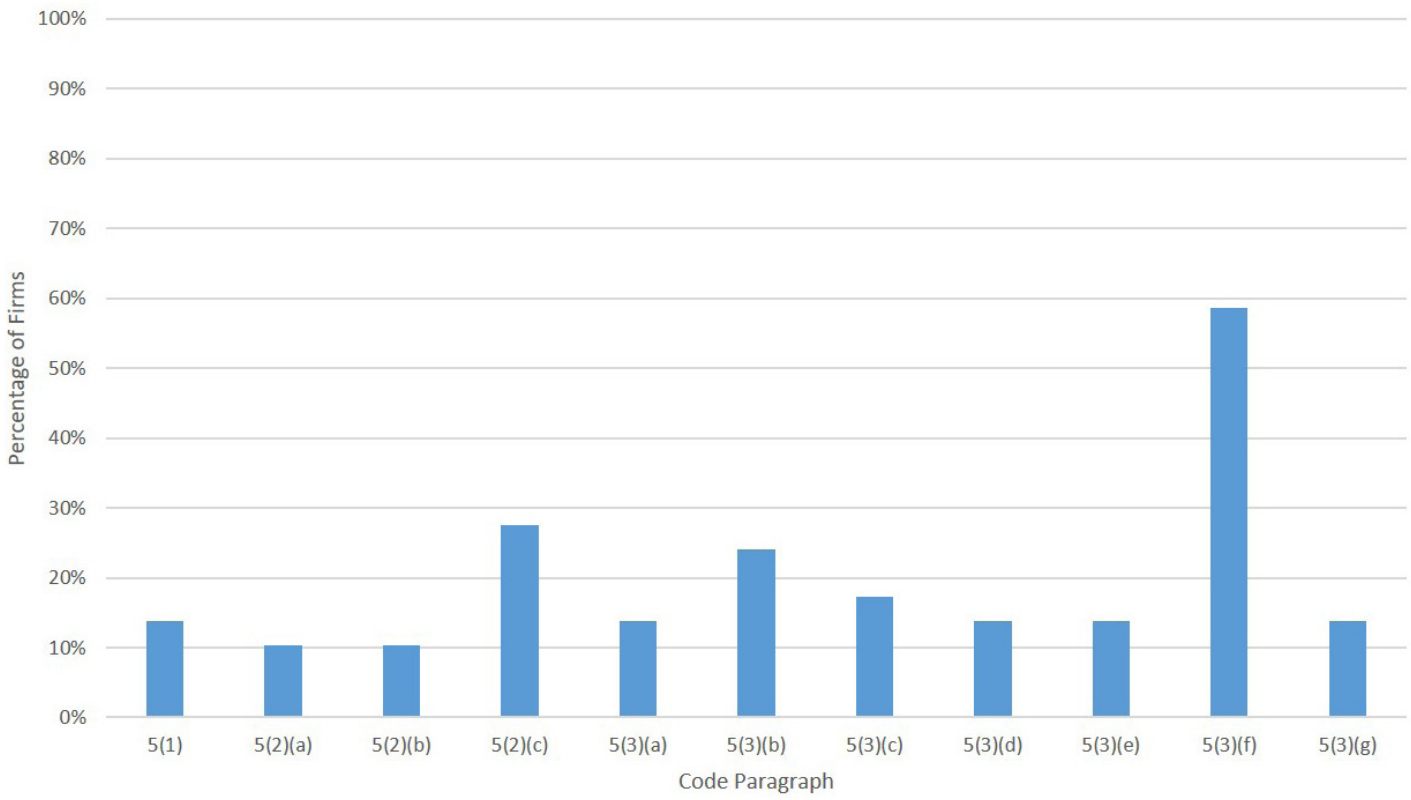
>>> a group BRA being used which was not tailored to the firm. Group BRAs might be possible, but must still reflect the different risk elements and assessment of the different activities undertaken by regulated or supervised legal entities in the group, the jurisdictions covered, and meet the IoM Code obligations for IoM entities covered by the group BRA;

>>> several BRAs were reviewed which had listed risk areas to be considered from the Code or the Handbook, but contained no evidence of them being considered, assessed, recorded, or mitigated as is required;

>>> BRAs which referred to outdated legislation, NRA or Handbooks, and had not been reviewed or maintained; and

>>> a high number of BRAs did not pay heed to the information and results from individual CRAs. For instance, not providing a commentary of the proportion of customer base that are foreign PEPs and detailing the risks these customers present.

Areas of paragraph 5 of the Code contravened



6.2.3 Customer risk assessment

A lack of, or inadequate CRAs. Inspection findings included:

>>> no individual CRAs completed or no evidence of having individual CRAs. In one case, the "CRA" was an overview of customer types and associated risks which appeared to be part of the wider BRA;

>>> CRAs and processes for "newer" customers only. Where a revised CRA had been introduced it was not applied to historic customers resulting in an inconsistent picture of risk across the customer base;

>>> initial CRAs not reviewed or updated since their creation at the on-boarding stage;

>>> scoring systems used without context or instructions. No evidence of consideration or reason for scoring;

>>> scoring systems failed to consider Code mandated risk factors or failed to increase score when considering PEP customers;

>>> scoring systems, or manual amendments, discounted customer risks (even when significant adverse media evidence existed);

>>> where a UBO was assessed as higher risk but associated structures had a separate, lower risk rating with no clear explanation or rationale. Not taking into consideration the complex structure(s) involved and recognising potentially linked risk factors;

>>> no procedures for carrying out CRAs;

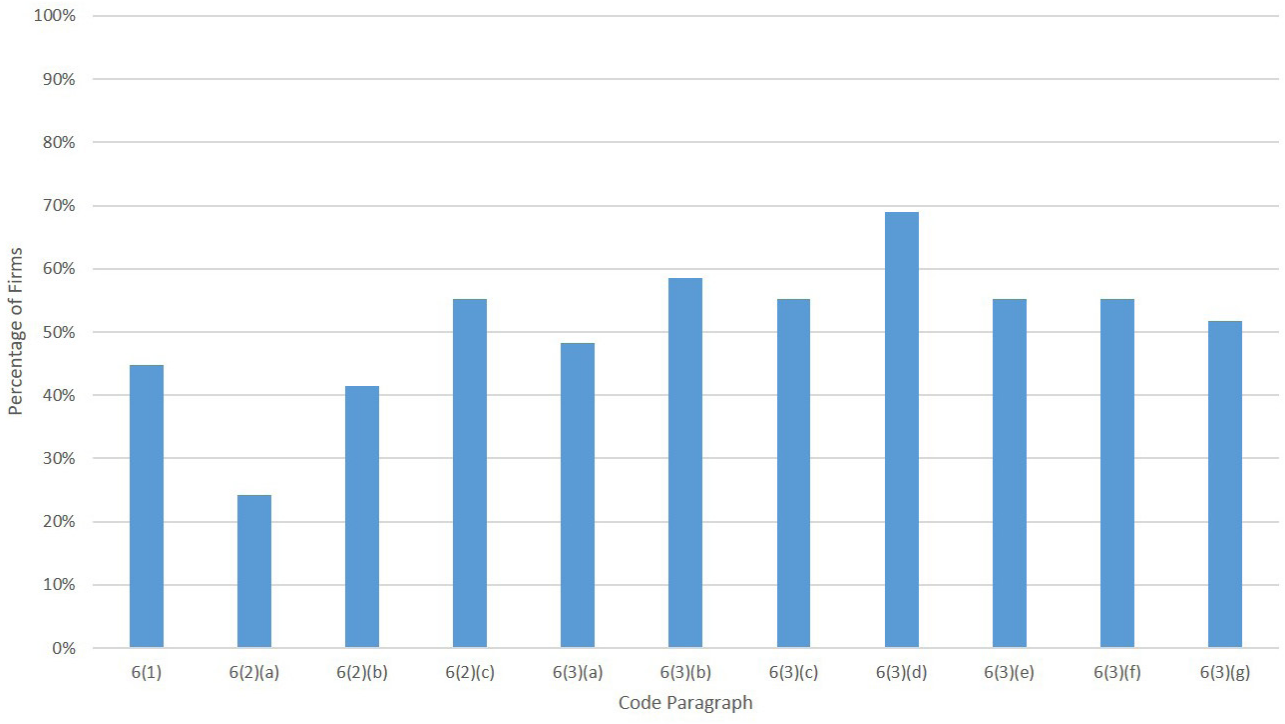
>>> CRAs with no methodology or basis for rating risk factors, leading to an overly subjective and inconsistent approach. Many were seen to solely consider the jurisdiction of the PEP without considering other risk factors, for example the PEP's role;

>>> the location used in risking was the country where the PEP's assets tended to be located rather than the home country where they were a PEP or their normal country of residence;

>>> acceptance of customer assertions that significant adverse media was politically motivated, and was therefore untrue; and

>>> reliance on introducers where no risk assessment of the introducer has been undertaken.

Areas of paragraph 6 of the Code contravened



6.2.4 Identifying PEPs and on-boarding of PEPs

Weaknesses or gaps were found in relation to identifying and on-boarding PEPs. Inspection findings included:

>>> lack of senior management consideration or approval for the acceptance of proposed PEP customers[9], or once customers became PEPs during the lifecycle of the business relationship;

>>> PEPs not identified by screening at on-boarding, but were identified by later manual checks on the same, or very similar, evidence;

>>> failure to identify customers/family/associates as PEPs;

>>> documents being accepted which differed from the firm's policies or procedures without an explanation as to why they were accepted;

>>> discounting individuals flagged in screening as PEPs for minor detail discrepancies;

>>> not documenting consideration of adverse media and why it has been disregarded;

>>> untranslated documents being used to identify the PEP, but no commentary as to why the document has not been translated and what customer information the document is verifying;

>>> high risk PEPs on-boarded, but not reflected in the CRA, BRA, or controls. This was even observed as occurring within firms who said that they would not on-board high risk PEPs; and

>>> treating source of funds ("SOF") as source of wealth ("SOW") resulting in no SOW or evidence obtained for PEPs. For example:

- some considered only the account used to make payments as the SOF;
- some captured the actual source of the funds paying for the transaction/ product involved as being the source of customer wealth;
- one stated SOF as the loan that was the product being supplied to the PEP; and
- some had nothing on the source of the foreign PEP's wealth.

6.2.5 Ongoing monitoring of PEPs

Weaknesses or gaps were identified in relation to ongoing monitoring and checks. Inspection findings included:

>>> not reviewing PEPs on a frequent basis, or the periodic review cycle failed to keep up with the timescales quoted in policies and procedures;

>>> unidentified PEPs spotted at later review, and the need for additional requirements noted, but flagged to be done "at next trigger event";

>>> only customer-notified changes generated a "trigger event". Or no trigger event apparent for multiple years/to date;

>>> monitoring limited to checking identity evidence (for example, passports) had not expired. No enhanced monitoring or due diligence of foreign PEPs. Not revisiting SOF / SOW over time;

>>> no enhanced approach. The same monitoring/ controls/checks applied to all customers including foreign PEPs; and

>>> failure to carry out screening checks sufficient to identify people who became PEPs after they were on-boarded or had new adverse media.

[9] Or individuals connected to customers

Weaker controls and gaps in reviews appeared to be more prevalent in low transaction products and areas, such as single premium/paid up investment products despite obligations to review regularly.

Low risk does not mean no reviews are necessary, but that the reviews should be tailored to the identified ML/FT risk.

The frequency and depth of the review and testing for a standard risk customer as part of ongoing monitoring/CRA refresh is expected to look different to that for a higher risk foreign PEP.

6.2.6 Sectoral findings

>>> Banks did not tend to have contraventions in relation to BRAs or in compliance testing. Weaker areas included enhanced PEP measures/ECDD and in CRAs.

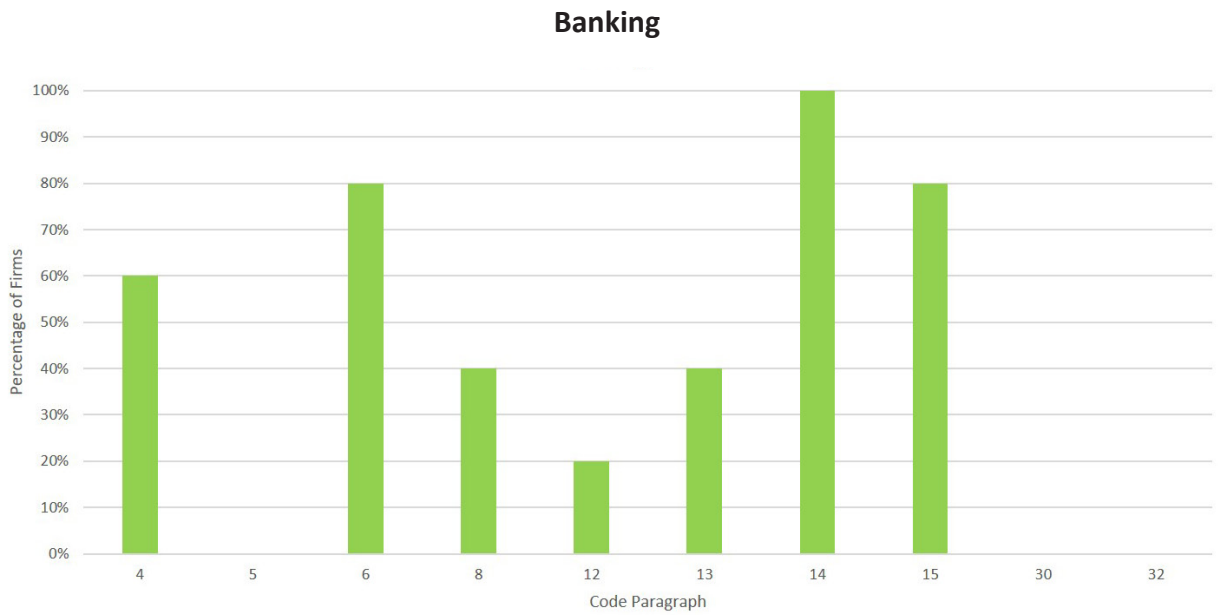
>>> Fiduciaries (TCSPs) were weaker in areas such as CRAs, policies and procedures, having enhanced PEP measures, ongoing monitoring and BRAs. A further area of note for this sector was to ensure any screening includes the client company or trust itself, as well as funding parties and other connected individuals.

>>> Insurance and Pensions firms as a group were weakest in CRAs and enhanced PEP measures ECDD. In several cases it was found that the firm had identified ECDD was required for a customer, however this was noted as to be followed up at the next trigger event. The Code does not permit deferral of undertaking ECDD, it must be undertaken at the time it is identified as being required.

>>> Investment and Funds key weaknesses were across policies and procedures, CRAs, on-boarding new business relationships and enhanced measures for PEPs/enhanced CDD. They also had some weaknesses in BRAs.

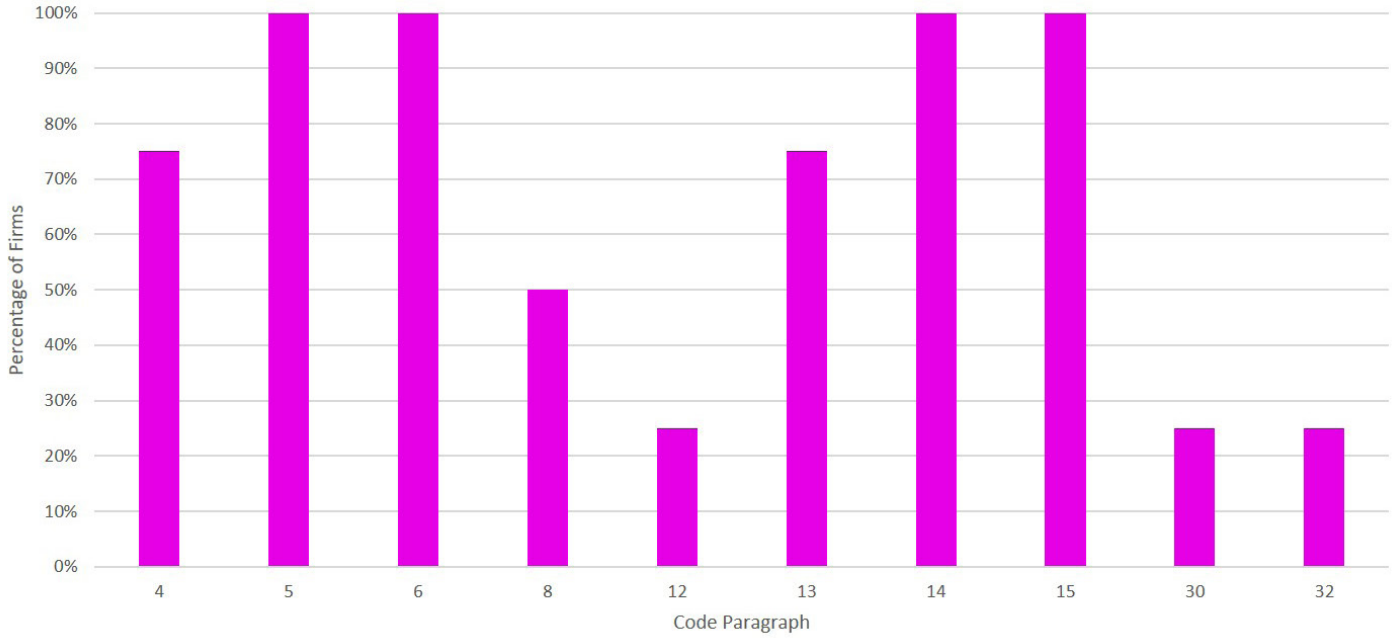
>>> Designated businesses' key weaknesses ranged across policies and procedures, BRAs, CRAs, enhanced PEP measures and compliance regime testing and assurance.

Comparison of code contravention by sector[10]

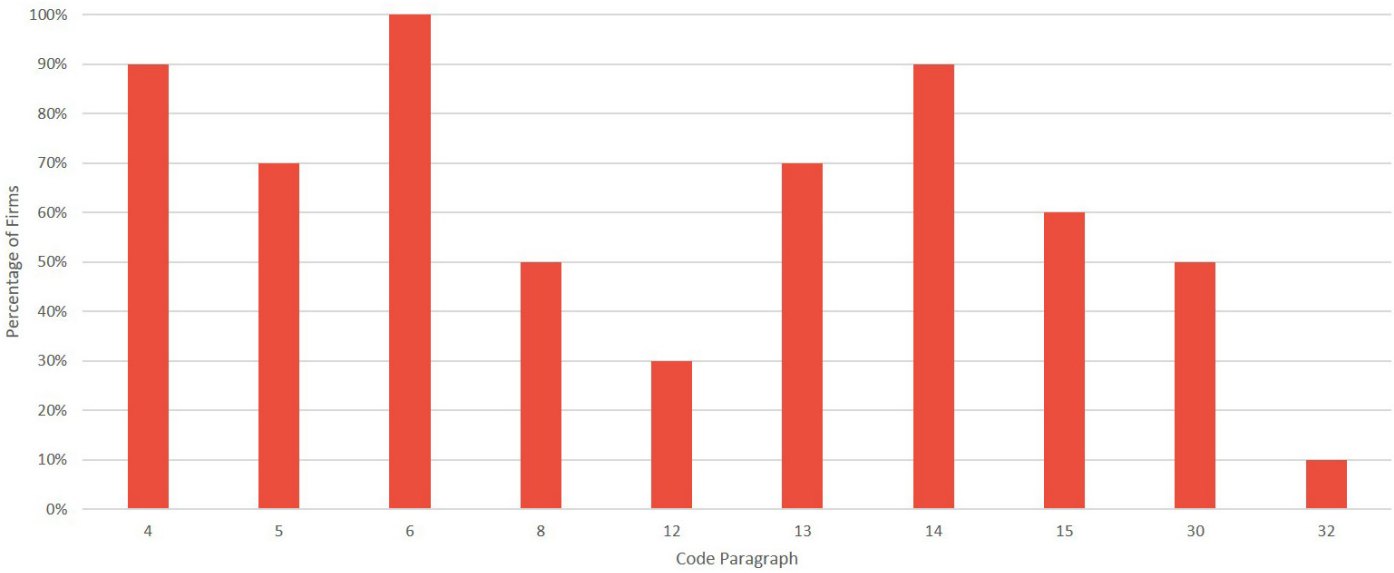


[10] These charts include the main paragraphs contravened, as identified by the Authority's inspection reports, not all Code paragraphs considered on inspections. Paragraphs 9, 10, 11, 19, 22, 33, 34, 35 are omitted from the chart. In addition, it is important to note differing numbers of inspections took place across sectors, with the fiduciary sector having the most inspections during the thematic exercise.

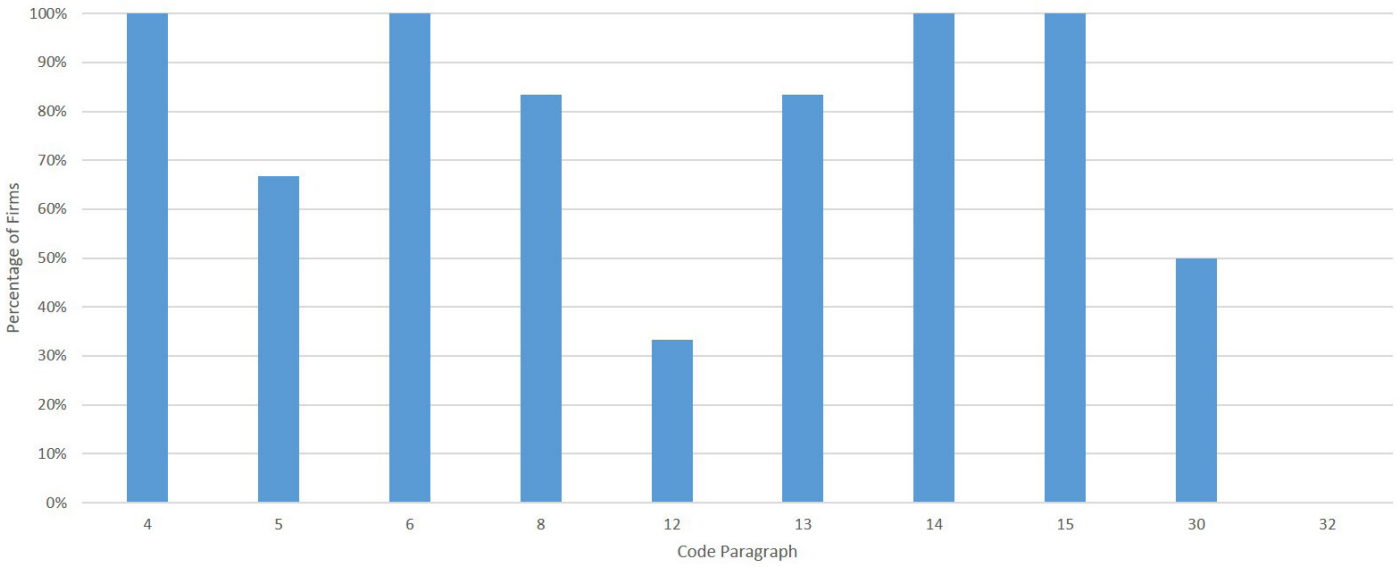
Life insurance



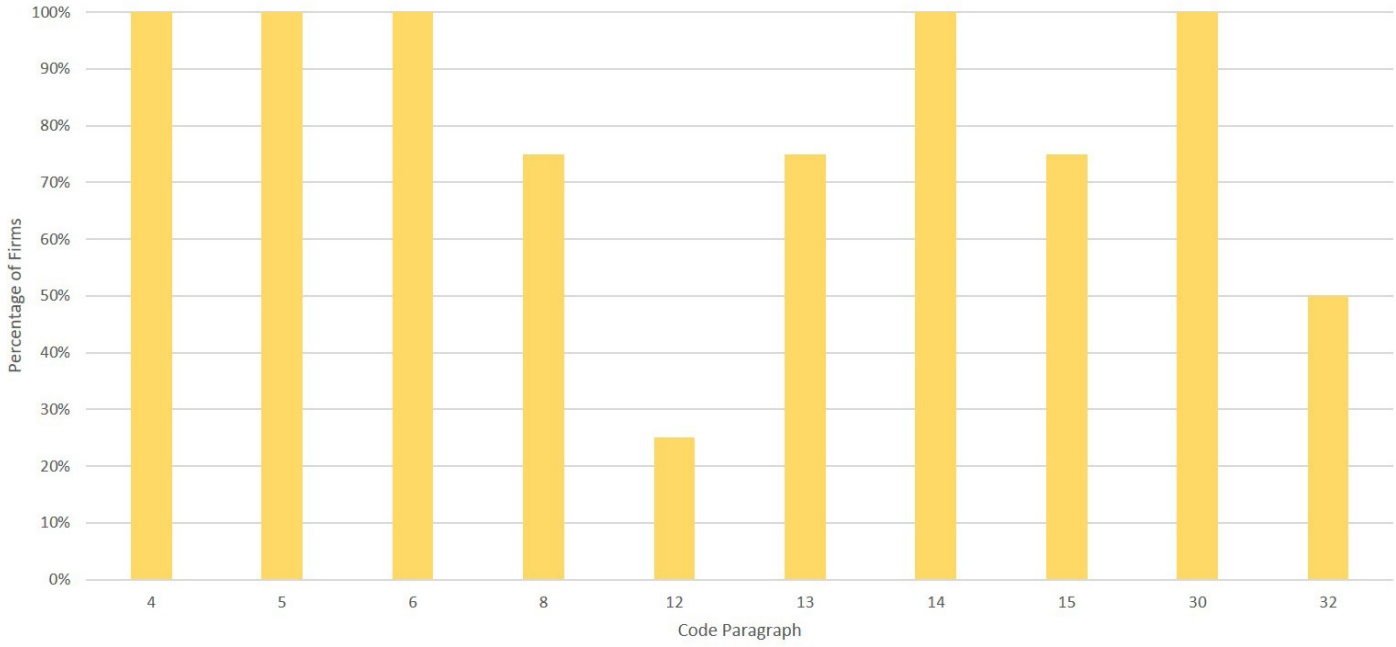
Fiduciary



Funds / Investment Business / Pension



Designated Business



6.3 Other findings

6.3.1 Training

Most firms provided some AML/CFT training for staff each year, although the number who provided AML/CFT training with PEP specific elements to staff whose work involved PEPs was lower. Findings from Phase 2 indicated 86% of firms had appropriate training in relation to PEPs.

6.3.2 Assurance reviews

A small number of firms had carried out an assurance review of their management and control of foreign PEPs/PEPs prior to the on-site fieldwork and had identified gaps and weaknesses themselves. In most of these cases, the firm had developed a remediation plan, and had started remediation work prior to the inspection. It appeared likely from the review dates that much of the work was instigated by the announcement of the Authority's foreign PEP thematic exercise.

In some cases the firm's assurance testing had not noticed widespread failures to follow the firm's procedures. Also, the compliance team often carried out first line AML/CFT checks and there was no independent testing or reporting on how well the firm's procedures and controls were being carried out.

Where foreign PEPs are prevalent in the customer base of a firm, this is a key risk environment to the firm and as such should be a key topic for both senior management reporting and assurance testing of a firm.

> *In some cases assurance testing had not noticed widespread failures to follow the firm's procedures*

6.3.3 Recording of PEP status

In one firm a 'belt and braces' approach was taken in counting anyone or any entity who had even a remote connection to a PEP. Another firm still counted people who were no longer in a business relationship in their PEP numbers.

In both cases the inclusion of historic customers, non-PEP individuals, and legal persons (who cannot be PEPs) gave a false (higher risk) picture of the PEP risks faced by the business and result in additional Code obligations that the firm is required to comply with.

These higher numbers influenced the risk-based inclusion of these firms in the thematic exercise, in both Phase 1 and 2.

Firms that continued to count PEPs from business relationships which had ceased included those where the insurance policy had ceased or run its course, or the firm had ceased to act for the customer some time ago[11].

All firms involved in the thematic exercise had a PEP register. However, on some PEP registers reviewed the reason why a customer had been determined to be a PEP was often not recorded.

This is recommended good practice to enable a user of the PEP register to understand at the outset the rationale/reason someone is a PEP, which will further assist in considering customer risk. Other areas to record could include:

- date identified as a PEP;
- method by which identified;
- who signed off on the PEP status;
- when was the last periodic review and when is the next review scheduled.

[11] The data reported by firms at Phase 1 has not been corrected as a result of the Phase 2 inspection findings and should therefore be seen as indicative, but not a completely accurate reflection of PEP numbers.

7. Approach to the exercise

The Authority analysed the Phase 1 data from firms, including:

>>> the spread of the numbers of foreign PEPs and proportions within firms;

>>> the nature of the PEP role;

>>> PEP nationality and location;

>>> the risk rating ranges applied; and

>>> external disclosure rates and how many PEP relationships were declined.

The Authority also had visibility of PEP numbers from year on year AML/CFT statistical returns from firms, and information from any prior supervisory inspections. From this, 29 firms were selected for inspection ("Phase 2") during 2022.

In advance of the focused inspections, firms submitted detailed procedures and controls, including CRA methodology and their BRA. These were subject to desk-based reviews, and the inspections tested how they were applied in practice. Testing included examinations of samples of customer files and records[12]. In all cases, detailed on-site fieldwork[13] or a desk-based review[14] took place, and firms received individual inspection reports.

In a number of cases it was identified by the Authority that the firm was not ready for the inspection, or the Authority's officers could not access all of the customer file documentation while on-site, meaning a full review could not be undertaken at the scheduled time. It is essential firms are prepared for an on-site inspection and all documents and information is accessible.

7.1 Objectives of the inspections

Inspections, which focused on firms' approach to foreign PEPs, had the same core objectives –

Objective 1: review the business risk assessment (Code paragraph 5), determine the approach/risk appetite in relation to foreign PEPs, and assess its effectiveness in practice.

Objective 2: review the customer risk assessments (Code paragraph 6), focusing on the methodology used where the customer is a foreign PEP and assess its effectiveness in practice.

Objective 3: review the business' policies and procedures in order to understand how foreign PEPs are identified (Code paragraph 14) and on-boarded (Code paragraph 8). Also to assess their effectiveness in practice.

Objective 4: review the business' policies and procedures in relation to ongoing and enhanced monitoring of foreign PEPs (Code paragraphs 13 and 14). Assess the effectiveness of those policies and procedures in practice. Consider the effectiveness of screening and ongoing monitoring, including identifying PEPs once the relationship has been established.

Objective 5: review of the results of quality assurance/reporting to the Board and testing in relation to foreign PEPs to assess the adequacy of governance and risk management in relation to foreign PEPs (Code paragraph 30).

Objective 6: review the business' policies, procedures and training registers in relation to staff training in relation to foreign PEPs (Code paragraph 32).

Paragraphs 12 and 15 of the Code (Beneficial Ownership and Enhanced Customer Due Diligence) were also considered where appropriate.

[12] Each sample was selected and communicated to the firm with two business days' notice.
[13] 27 firms
[14] 2 firms

7.2 Inspection reporting

Formal inspection reports were produced for each inspection. Written on an exception only basis, the reports set out the findings of any weaknesses or contraventions in relation to the Code. This is in line with the Authority's published guidance on inspections.

With an emphasis on exceptions, the reports do not detail areas where the firm is Code compliant, other than to say 'no contraventions were found' in relevant Code areas. In part, this is because the nature of the inspections (thematic and focused) meant that the Authority's officers did not examine or test beyond this limited range, and so could not comment on the firm's wider compliance with the Code across its wider customer population or activities.

Some firms found the nature of the reports unsettling. It is important to note that these reports are only issued to the firm involved, and the Authority will not be publishing the reports or detailed findings from each inspection in this document.

Each report was internally peer reviewed, and draft reports were shared with the firm for fact checking to inform the final inspection report.

Where weaknesses or contraventions were identified, the firm has to consider, propose, and deliver a plan regarding remedial actions to bring the firm into Code compliance.

With a broad understanding of standards resulting from the 29 firms inspected, inspections with significant or material Code contraventions were referred to a Governance Panel of the Authority.

This Governance Panel considered the outcomes of those inspections, areas which required remediation, and whether the case justified consideration by the Enforcement Division of the Authority. A number of firms were referred by the Governance Panel for consideration by the Enforcement Division at the date of this report[15].

[15] Some cases remain under/are pending review and/or referral.

8. Glossary of terms

TERM	MEANING IN THIS REPORT
AML/CFT	Anti-Money Laundering/Countering the Financing of Terrorism
BRA	Business Risk Assessment
CDD	Customer Due Diligence
CODE OR AML/CFT CODE	The AML/CFT Code 2019
CRA	Customer Risk Assessment
DESIGNATED OR REGISTERED	Refers to designated non-financial businesses, firms or entities required to be registered for AML/CFT Code supervision under the Designated Businesses (Registration and Oversight) Act 2015
ECDD	Enhanced Customer Due Diligence
HANDBOOK	The Authority's AML/CFT Handbook
IoM or ISLAND	Isle of Man
ML/FT	Money Laundering/Financing of Terrorism where reference is made to ML/FT this also includes targeted financial sanctions and proliferation financing
NRA	National Risk Assessment
PEP	Politically Exposed Person
REGULATED	Refers to firms regulated under the Financial Services Act 2008 or the Insurance Act 2008
RELEVANT ENTITIES OR FIRMS	Refers to regulated or designated/registered businesses
SOF	Source of Funds
SOW	Source of Wealth
THE AUTHORITY	The Isle of Man Financial Services Authority
TRA	Technology Risk Assessment
UNODC	United Nations Office on Drugs and Crime

Appendix A - What is a PEP?

A Politically Exposed Person is any person who is (or has been) entrusted with prominent public functions, or is related to, or a close associate of, such a person. This is defined in the Code. Due to their position and influence, many PEPs are in positions that could potentially be abused.

PEP risk includes offences such as corruption and bribery, as well as activity related to FT. There are ML risks associated with any benefits that may accrue from such abuse of position.

Approximately 17% of matters currently with the Economic Crime Unit concern bribery or corruption. That threat arises substantially from those seeking to launder proceeds of these offences through the IoM, rather than from domestic predicate offences.

PEPs include:

>>> head of state, head of government, minister or deputy or assistant minister;

>>> senior government officials;

>>> member of parliament;

>>> senior politician;

>>> important political party officials; and

>>> others such as high ranking members of the judiciary, armed forces, international bodies or state owned enterprises[16]

"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.

The NRA further mentions that this may involve PEPs directly or indirectly through introducers, intermediaries or complex structures.

The Authority's Handbook states –

"Corruption is a complex social, political and economic phenomenon that affects all countries. Corruption undermines democratic institutions, slows economic development and contributes to 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 standards, or where they do not meet financial transparency standards. Relevant persons should take appropriate measures to mitigate those risks."

[16] As defined in paragraph 3 of the Code

In recent years, there has been much more publicity on the subject of international PEP risks as instigated by the Pandora, Paradise, Luanda, and FinCEN leaks/ papers. This has been supplemented in regular media articles by organisations such as Transparency International, the International Consortium of Investigative Journalists, the Organized Crime and Reporting Project and others, many mentioning foreign PEPs.

Although not in a position to comment on the legality or illegality within the media stories, it is clear that there are concerns and queries raised on how some PEPs actually obtained their wealth and how they have it managed.

Allegations include PEPs or family members or associates of PEPs:

>>> with individual wealth that appears unlikely considering their official salary or income over their career;

>>> gaining ownership of land, telecoms, oil or mining rights below true value, but delivering significant profits and huge personal wealth;

>>> using state funds or subsidies or third country contributions intended for aid/ development funds to accrue personal assets;

>>> assigning [or persuading others to assign] rights to others/third countries in return for personal funds/ bribes; and

>>> receiving these third party payments into accounts or structures outside their home country, avoiding domestic scrutiny or legal restrictions on banking, funding or capital movements.

Although the project started long before the Russian invasion of Ukraine, the resulting sanctions of businesses and individuals, including some PEPs, and related media articles have again highlighted possible foreign PEP risks.

FATF guidance and recommendations, as well as the IoM's own AML/CFT Code and guidance, set out additional requirements and expectations on firms for business relationships connected to PEPs. These are preventive in nature, and although they are needed because of the possible higher risk of PEPs, they are not to be interpreted as meaning that all PEPs are involved in criminal activity.

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