Isle of Man Government

National Risk Assessment of Money Laundering and the Financing of Terrorism

Cabinet Office/Oik Coonceil ny Shirveishee
January 2020

Contents

Introduction by the Chief Secretary, Chair of the Financial Crime Strategic Board

This is the second national risk assessment (NRA) of money laundering and terrorist financing (ML/TF) risk conducted by the Isle of Man (IoM). The NRA aim is to identify, understand and evaluate the risks faced by the IoM and highlight areas where action is required. These actions are incorporated into a national Financial Crime Strategy which is agreed and adopted by government and overseen by the Financial Crime Strategic Board.

Undertaking an NRA is a core requirement of the Financial Action Task Force (FATF), the international body responsible for setting and reviewing global standards for anti-money laundering and countering the financing of terrorism and the proliferation of weapons of mass destruction (AML/CFT). The FATF 40 Recommendations provide the international standards which all countries are expected to meet; it is IoM Government policy to adhere closely to these recommendations.

A key finding of the NRA conducted in 2015 was that the IoM needed to improve in areas such as financial intelligence, financial crime investigation and asset recovery and this has been the focus for work over the past four years. These findings were echoed in the conclusions of the MONEYVAL (a Council of Europe Committee)[1] evaluation of the IoM in 2016. The MONEYVAL evaluation found that the IoM had a strong AML/CFT framework, but that improvements were needed, notably in the effectiveness with which the authorities identified and pursued potential ML/TF cases and confiscated the proceeds of crime. Work to address the recommendations made by MONEYVAL is ongoing and the findings of that report have informed this latest NRA.

The IoM Government, having adopted this NRA, has directed the Financial Crime Strategic Board to draft a new Financial Crime Strategy for 2020-2023 and report upon the delivery of the actions and outcomes identified therein.

[1] The Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism (MONEYVAL) is a FATF-style regional body which undertakes peer reviews of its members.

1. The 2020 Risk Assessment: Executive Summary

This NRA builds upon the 2015 NRA and the findings and recommendations of the MONEYVAL Mutual Evaluation Report of 2016. The 2020 assessment also has the benefit of access to other key public reports which were not available in 2015 including the supranational European Union Risk Assessment and the 2015 and 2017 risk assessments of the United Kingdom (the largest trading partner for the IoM). The assessment has been conducted with cross-government participation, including law enforcement agencies, the Financial Intelligence Unit (FIU), industry regulators and the private sector.

The findings of the 2020 assessment concerning the overall level of risk for the IoM are that the ML risk remains Medium High and the TF risk as Medium Low.

The IoM is an international finance centre; the main threats to the IoM arise from international ML, where the wide range of financial and non-financial services available in the IoM may be used to launder the proceeds derived from foreign predicate offending. The types of services provided in the IoM, although fairly generic in nature, may be used to conceal the proceeds of crime or to conceal or disguise the origins of those proceeds, through international transfers of funds and the use of complex corporate structures. Criminals may also seek to use jurisdictions which are stable and which have an established rule of law in order to protect their assets; this presents a further risk for the IoM.

The breadth of services available in the IoM, which provides international banking, tax structuring, company and trust formation, investment in real estate and registration of yachts and aircraft within one jurisdiction, may also be attractive to those seeking to disguise and to benefit from the proceeds of corruption through, for example, investment in high end assets. Cross-sectoral risks in the IoM arise from a number of sources including the rapid development and introduction of new technologies, the increasing use of digital currencies, de-risking and the Island's economic model which is aimed at attracting financial and related business from corporations, high net worth individuals, etc.

The objective of the authorities is to take an informed and proactive approach to preventing and detecting ML and TF in response to the risks identified. Banks, and other sectors and individuals providing services to companies and trusts established in the IoM, including company incorporation, should be particularly aware of the threats and vulnerabilities identified in the NRA and the need for reporting suspicions promptly and fully to the FIU. In summary, the authorities and industry must work collaboratively together to protect the IoM from being used to launder criminal and terrorist finances and it is a role of Government to foster this united approach. Financial Institutions (FIs) and Designated Non-Financial Businesses and Professions (DNFBPs) should consult the NRA when undertaking their own assessments of risk.

Key findings:

The products and services available in the IoM have not altered significantly since the 2015 NRA. New data confirms the findings of the 2015 assessment and is also providing regulators with a more in-depth understanding of each sector and how sectoral risks relate to each other.

a. The reforms introduced by government, including increased investment, are taking effect. The reforms have been underpinned by strategy, policy and procedural development enabling the authorities to work together in a more collaborative and

effective manner. Effective use needs to be made of new powers, procedures and resources that have been allocated to the authorities.

b. Investment in developing expert knowledge, skills and specialist training to support the pursuit and positive resolution of ML and TF cases needs to continue.
c. The authorities now have better data available to them; full analyses and understanding of the data will enable it to be used effectively to inform risk-based supervision at sector and firm level, preventive work and law enforcement activities.
d. The Regulators, the IOM Financial Services Authority (IOMFSA) and the Gambling Supervision Commission (GSC) need to continue regular, risk based supervision of AML/CFT with obliged entities to ensure compliance with the new AML/CFT Codes introduced in 2019. Businesses carrying on designated business activities which are not registered with the IOMFSA are investigated and dealt with appropriately.
e. The accuracy of the Beneficial Ownership database is tested by the IOMFSA using a risk-based approach; however the accuracy and completeness of identity and verification details on registration need to be reviewed.
f. The impact of the UK exit from the EU is currently unknown; the authorities will need to monitor and take appropriate action where necessary. This includes taking action when required to address changes to the AML/CFT regime e.g. implementation of international (UN) sanctions.
g. A continued focus on the quality of border controls in respect of cash movements, including training, facilities for declarations, reporting of suspicions to the FIU, etc. is required. A process to ensure data on all cash seizures (whether at the border or elsewhere) is captured needs to be established.

Data and intelligence

Collection and analyses of statistics and information from industry, including data on financial flows is continuing. Particular focus is being given to the transfers of funds to and from higher risk jurisdictions. This data will be used to enhance risk-based supervision within and across entities overseen by the IOMFSA for AML/CFT measures. The IoM will continue to take account of emerging risks and new typologies, in particular in relation to virtual currency and to online gaming (the latter representing the largest economic sector in the IoM). A centralised database of Beneficial Ownership was introduced in 2017; law enforcement including the International Cooperation and Asset Recovery Team (ICART), the FIU, and competent authorities all have direct access to the database.

Investigation and asset recovery

There has been a significant increase in casework for the Economic Crime Unit (ECU) from 34 cases in 2016/17 to 90 in 2018/19; the main predicate crimes for ML continue to be fraud, false accounting and deception. Two-thirds of the cases being investigated by the Economic Crime Unit (ECU) arise from predicate offending outside the IoM. A number of significant cases concerning foreign predicate criminality have yet to be referred for prosecution. High levels of international engagement are being evidenced by the ECU in pursuit of investigations. However some responses to outgoing letters of request issued by the IoM have been extremely slow which is frustrating progress in ongoing cases.

The ICART has had a number of successes in using previously untested powers under POCA and other legislation. It has also restrained some large sums; however Restraint Orders concerning two significant cases were discharged by the Court during 2018.

Further development in developing technologies, including Convertible Virtual Currencies (CVCs)[2] and related products, are creating new challenges for supervisors and law enforcement. This is the case with many jurisdictions.

TF and Sanctions

Reporting on potential breaches of international financial sanctions has been streamlined, with all reports now made to the FIU. The Customs and Excise Division of Treasury (CED) is engaging with the UK's Office of Financial Sanctions Implementation (OFSI) new 'Virtual Sanctions Network' which has the aim of promoting dialogue and cooperation between the UK, the Crown Dependencies and the Overseas Territories.

Supervision and Preventive Work

The merger in 2015 of the Insurance and Pensions Authority and the Financial Supervision Commission, to form the IOMFSA, is enabling the delivery of a consistent supervisory approach. This is enhanced by closer working between the IOMFSA and the GSC e.g. on the new AML/CFT Codes which were made in 2019.

Non-face to face business is a significant feature of business in the IoM as an IFC. MONEYVAL made a number of recommendations regarding use of intermediaries that introduce customers and controls, around evidence of identity. New legal requirements have been introduced and must be implemented effectively by industry.

Tax

The Income Tax Division (ITD) has implemented, and is continuing to implement, commitments to the new global standards on transparency and exchange of information for tax purposes as well as those designed to address Base Erosion and Profit Shifting (BEPS). The sharing of intelligence which is generated through international requests made under international agreements, including Tax Information Exchange Agreements (TIEAs), continues to present a challenge. International requests concerning tax are made directly to ITD; this information is confidential to the tax authorities[3].

Borders and International

The planned departure of the UK from the EU will impact upon the IoM since the Island's limited relationship with the EU (including participation in the customs union) exists as an adjunct to that of the UK. The effect on ML and TF matters requires careful monitoring. The quality of the Island's border controls was identified as an issue by MONEYVAL in 2016, in respect of risks for controls on cash and similar instruments. The authorities have undertaken further risk assessments and, whilst this area is not currently viewed as a significant risk, the position will continue to be actively monitored.

[2] In 2018 the FATF adopted the term 'virtual assets' which encompasses virtual currency and other digital assets, however relevant IoM legislation refers to 'convertible virtual currency' and so this terms has been retained in the NRA.

[3] Under the terms of international agreements and in accordance with international tax standards"

Sectoral Contribution to IoM National Income

The following table summarises details concerning the size of each sector in the IoM, where dis-aggregated information is available.

Table 1: Sector contribution to national income and related information

Sector	Size[4]	No. of employees	No. of jobs	% National Income 2017/18
Banking	38,800	2212	2210	6%
Insurance (Life & Non-Life)	75,380	1981 (341 & 1640)	1977	17.6%
Online Gaming	190,000	800	796	21%
Financial & Other Business Services[5]	27,498[6]	3243	3204	8%
Other Professional Services (including Money Transmission Services & Consultants)		1472	1487	4.9%
Legal Services		587[7]	582	0.83%
Accountancy Services		652	644	0.94%
Corporate Service Providers	250,098	1797	1820	3.1%
Pensions	11,000	187		0.16%
Payroll		102		0.0009%

[4] Assets under Management (AUM) in millions £

[5] This includes three subsectors: Other Financial Services/Other Business Services/Property Investment. Property Investment is made up of three sub-categories: Property owning management/Estate Agents/Commercial Property Letting)

[6] AUM for funds and investment business

[7] All jobs in the legal sector, inclusive of lawyers and non-legal staff

Summary of Overall Risk Ratings by Sector

The following table summarises the overall ML and TF risk ratings assigned to each sector by the authorities. More detailed information on each sector can be found within this report.

Table 2: Summary of overall risk ratings by sector[8]

Sector	ML Risk	TF Risk
Banking	Medium	Medium
Collective Investment Schemes, Fund Managers & Administrators	Medium	Medium
Asset and Investment Management	Medium	Medium
Financial Advisory	Low	Low
Life Insurance	Medium	Medium
Non-Life Insurance	Medium Low	Medium Low
Pensions	Medium Low	Medium Low
Payment Services/e-money	Medium	Medium
Money Transmission Services (bureau de change / agency)	Medium Low	Medium Low
Credit Unions	Medium Low	Medium Low
Accountancy Services	Medium	Medium Low
Payroll	Medium	Low
Advocates	Medium	Low
Registered Legal Practitioners	Medium	Low
Online Gambling	Medium	Low
Terrestrial Gambling	Medium Low	Low
Trust and Corporate Services	Medium High	Medium
Convertible Virtual Currencies	Medium High	Medium
Real Estate Services	Medium	Low
Non Profit Organisations	Low	Low
Moneylending	Medium Low	Low
High Value Goods Dealers	Low	Low

[8] The overall risk ratings take into account the risks for each sector once domestic AML/CFT controls are applied.

2. Policy & Coordination

The Financial Crime Strategic Board (FCSB) is the strategic co-ordinating body in the IoM for AML/CFT. The FCSB, which reports directly into a Committee of the Council of Ministers (the National Strategy Group), is chaired by the Chief Secretary who is the senior civil servant and adviser to the Chief Minister[9]. The Board members include the chief officers of the Attorney General's Chambers (AGC); the Police; the FIU; CED; the two Regulators, (the IOMFSA and the GSC); ITD; the Department for Enterprise (DfE) and the Cabinet Office. The Board is responsible to the Council of Ministers[10] for making recommendations on AML/CFT policy and for the delivery of the Financial Crime Strategy.

A central AML/CFT Policy Office was established within the Cabinet Office by the Chief Secretary in 2016; the Policy Office works on behalf of the FCSB to ensure co-ordination of the AML/CFT regime across law enforcement authorities and regulators. The AML/CFT Policy Office team is led by the Head of AML/CFT Policy who reports regularly to the FCSB on progress made against relevant action plans, including the Financial Crime Strategy. The Policy Office undertakes a number of functions which include providing a central point of contact for MONEYVAL, ensuring that the IoM is represented in relevant international meetings on AML/CFT and coordinating the NRA process using the World Bank model. There are several other key groups which together contribute to AML/CFT policy development and coordination.

The Financial Crime Law Enforcement Effectiveness Group meets on a bi-monthly basis and is chaired by the Director of Financial and Cyber Crime. It was established in 2017 and aims to facilitate more effective working practices between law enforcement agencies. The Group complements an already existing Joint Tasking and Coordination Group, which coordinates and prioritises the national response to specific cases enhancing overall cooperation between the law enforcement agencies.

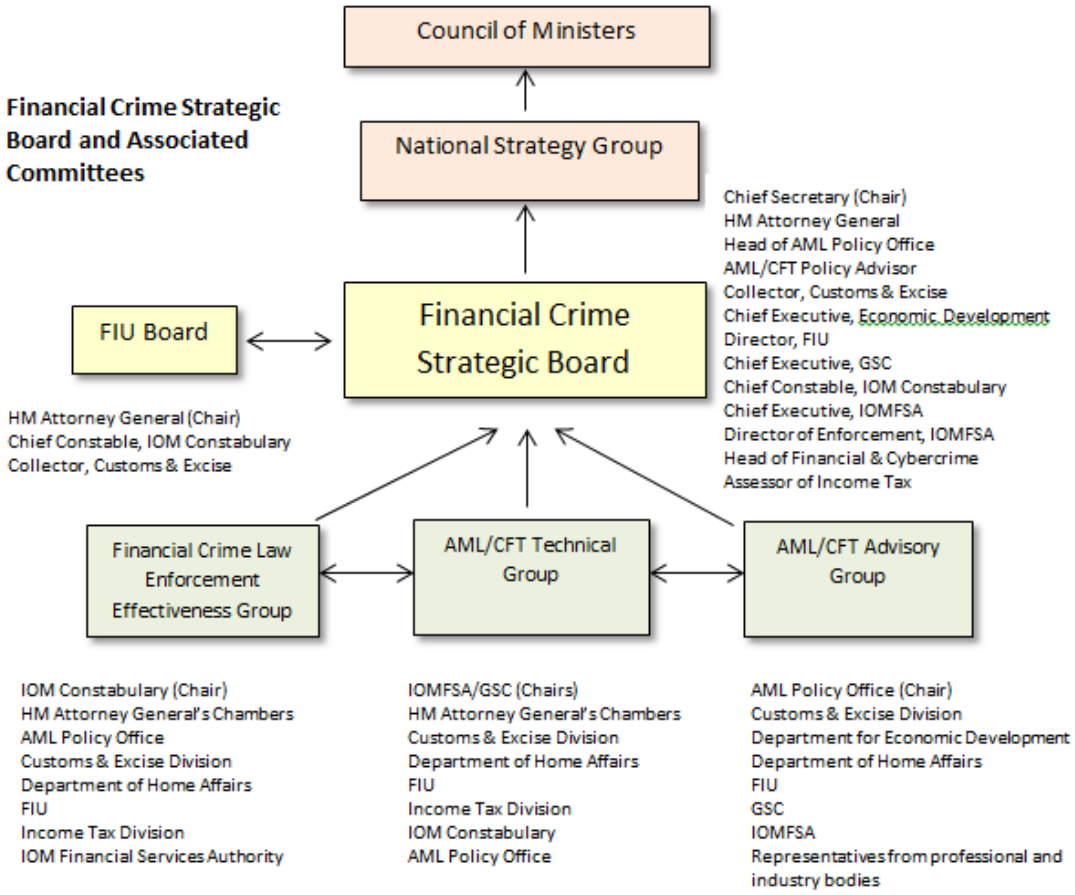
The AML/CFT Technical Group is a multi-agency group which meets regularly and is chaired alternately by each Regulator. The Technical Group provides a forum which facilitates cooperation and coordination on AML/CFT matters; it also monitors international standards and relevant guidance and provides information and advice to the FCSB. The FCSB from time to time tasks the Technical Group to review and report upon new or developing issues.

The AML/CFT Advisory Group meets quarterly and includes representatives from industry bodies. It is organised by the AML/CFT Policy Office. The meetings aim to strengthen communications, the exchange of financial intelligence and to facilitate cooperation between government, regulators and industry. The minutes of the meetings are published online to ensure the widest possible circulation.

A model of the reporting framework for AML/CFT policy and domestic cooperation is included below at Figure 1.

[9] The Chief Minister is the head of the elected Government in the IoM.
[10] The Council of Ministers is the Executive Government in the IoM, effectively the Cabinet.

Figure 1: Reporting Framework for AML/CFT Policy and Coordination



There is close collaboration between the groups, aided by the small size of government and relatively straightforward structure of the relevant authorities. In June 2017 the IoM published the Financial Crime Strategy 2017-2020. The strategy has four priority objectives, which are;

- Understanding the money laundering and financing terrorism threat, risks and harm facing the IoM.
- Ensuring that the IoM is a hostile jurisdiction for money laundering and the financing of terrorism.
- Pro-actively identifying and pursuing offenders: and
- Taking the benefit out of crime.

Each of the four priority objectives has a lead agency and progress against the strategy is periodically published by way of a report from the Cabinet Office.

There are a number of other relevant policies and strategies including the 'Proliferation and proliferation financing risk: policy protocol and the Combatting the Financing of Terrorism Strategy'. The AGC has also published several policy and strategic documents in relation to prosecuting financial crime and the work of the ICART. A number of these are published and available on the government website. Internally, the authorities have a series of MOUs (Memorandum of Understanding) in place and the required legal gateways for information sharing and to support multi-agency working.

The FIU is a member of the Egmont Group[11], the ICART and the ECU participate in CARIN[12] and the ECU works closely with, amongst others, the UK National Crime Agency and the City of London Police (Economic Crime Academy) and the Metropolitan Police Service Counter Terrorism Command.

3. The 2015 National Risk Assessment and the MONEYVAL Peer Review 2016

The first NRA for the IoM was finalised in 2015 and published in March 2016. The 2015 NRA concluded that the overall ML risk for the IoM was medium/high and that the overall TF risk was medium/low. The report identified fraud and tax evasion as the primary predicate offences for ML with the majority of these offences taking place outside the jurisdiction and the proceeds being laundered through the IoM. Proceeds from drug dealing and theft represented the primary domestic risk of ML. Domestic ML risk was significantly lower than international risk.

The international nature of the financial and non-financial services provided by firms based in the IoM and the close economic relationship with the United Kingdom, a global financial centre, was identified as presenting a higher level of ML risk. This was not considered to be the case in respect of TF as a significant number of key drivers for TF risk were only either minimally present, or not at all.

Key findings from the 2015 assessment were that:

- The IoM had a strong legislative framework in place for dealing with ML and TF.
- Domestic cooperation was good, the regulatory framework comprehensive and there was a high level of independence and integrity within law enforcement and the courts.
- There were weaknesses in the application of the AML/CFT framework, notably around law enforcement, financial intelligence and confiscation.
- No prosecutions for third party international ML had been undertaken since 2007 and the level of restraint of suspected proceeds and of confiscation was low.
- There were significant gaps in AML/CFT data both at national and at sectoral level.
- A registration and oversight regime for DNFBPs was due to be introduced but was not yet in place. This was not the case for trust and corporate service providers[13] (TCSPs) and gambling[14] as both sectors were fully supervised for AML/CFT and had been for a number of years.
- TCSPs were identified as having a medium/high risk of being used for ML; banking, securities and investments, insurance, accounting and gambling had a medium risk.
- Other Money Service Businesses and Lawyers (Advocates) were identified as a medium/low risk.
- Non-profit organisations (NPOs) including charities, digital currencies, Estate Agents and several other DNFBP sectors were not fully assessed owing to a lack of meaningful data.

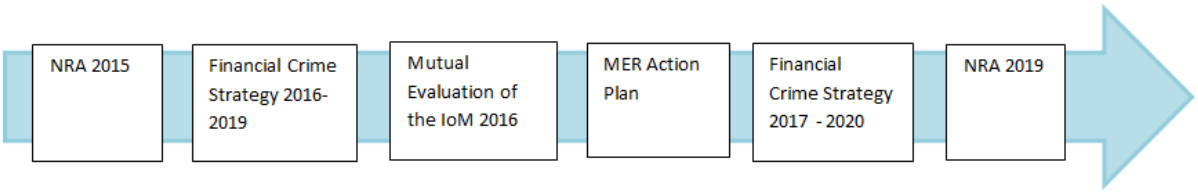
[11] Egmont is an international grouping of FIUs which seeks to promote the development of FIUs and cooperates in areas including information exchange, training and the sharing of expertise.
[12] CARIN is the Camden Asset Recovery Inter-Agency Network. It is an informal network of contacts and a cooperative group aimed at tackling the proceeds of crime.
[13] Corporate service providers have been subject to licencing and supervision for AML/CFT purposes since 2000 and trusts since 2005.
[14] The Gambling Supervision Commission oversees both online and terrestrial gambling.

A Financial Crime Strategy which aimed to address the issues identified in the NRA was adopted by government in 2016. The aims of the Strategy were overtaken by the recommended actions of the Mutual Evaluation Report (MER) of the IoM by MONEYVAL. The MONEYVAL report on the IoM, published in January 2017, concluded that;

- Coordination of AML/CFT policies was strong and that the 2015 NRA provided a thorough understanding of ML and TF vulnerabilities at national and sectoral level.
- A lack of data on incoming and outgoing flows of funds limited the understanding of threats in particular linked to TF.
- The FIU conducted only limited in-depth analysis of intelligence and the quality of SARs was low.
- The number of convictions for ML was modest and not reflective of the risk profile of the IoM. Very few parallel financial investigations had been conducted.
- Potential TF activities should have been more closely considered for possible investigation. Better awareness and a more proactive approach to potential suspicions of TF were needed.
- Mutual Legal Assistance was constructive and timely.
- FIs and DNFBPs applied a risk-based approach and demonstrated knowledge of AML/CFT. Insufficient knowledge of risk was demonstrated in respect of intermediary customers and where use was made of customer due diligence (CDD) supplied by intermediaries.
- FIs and DNFBPs were actively supervised but the legislative framework for DNFBPs was very new and there was no routine collection by supervisors of statistics to allow full consideration of ML/TF risk as a whole or at sector level.
- Although measures were in place to prevent misuse of legal persons and arrangements, it was common for TCSPs to not meet their customers (or the beneficial owners thereof) and to use professional intermediaries to collect and certify CDD information.

In total the MER made sixty-two recommendations to improve the effectiveness of the IoM in tackling ML/TF. These recommendations were incorporated into an action plan and have been priority areas of work for the IoM up to and including 2019. In light of the MER a revised and updated Financial Crime Strategy was adopted in 2017.

Figure 2 – Timeline on progress since the 2015 NRA



Strengthening the National Response to ML/TF

A key area identified for improvement in the 2015 NRA was the requirement for better quantitative and qualitative data at national and sectoral level to better inform the risk based approach for regulators, sectors and institutions. Progress made in this area includes;

- Data on the monetary value and volume of inflows and outflows for banks including origin and destination of funds is provided to, and analysed by, the IOMFSA, and shared with the FIU.
- The introduction by the IOMFSA of a detailed annual AML/CFT return which is completed by all regulated entities and the majority of DNFBPs.

- A legal requirement for gambling operators to provide AML/CFT returns to the GSC.
- The introduction of an on-line SAR reporting system in 2016.
- The introduction of a national end-to-end ML/TF reporting system in 2019.
- The continued development by the IOMFSA and GSC of a joint data system via which AML/CFT returns will be submitted by regulated entities, DNFBPs, and licenced operators.
- The introduction of new software into the ECU to assist with data mining and related activities.

Further enhancements to the AML/CFT legislative framework have taken place, including in respect of introduced business requirements.

Other improvements include a review and restructuring of the AML/CFT national oversight framework to strengthen domestic cooperation and strategic leadership and extensive work on developing and publishing AML/CFT strategies, policies, procedures and guidance across the authorities. This includes the establishment of a Cross-Border Cash Control Mechanism which clarifies the legislative powers, policy and operational process concerning the detection of falsely or undeclared cross-border movement of currency and Bearer Negotiable Instruments (BNIs) and the process for confiscation or seizure.

The quality of IoM border controls and the effectiveness of the customs regime on cash and BNIs were areas identified for improvement in 2015. Improvements were made in respect of inter-agency cooperation, notably more effective joint working between the police and Customs and training of security staff at the ports. A proactive approach by Customs in 2017/18 resulted in a 22% increase in the number of stops compared to the previous year. Legislation was also amended to extend the scope of powers of Customs officers to inspect premises for goods including cash.

In 2017/18 the IoM Government invested over £2.2 million in the FIU, ECU and the ICART. Over £500,000 was invested in a central AML/CFT Policy Office within the Cabinet Office, and development of a national AML/CFT Reporting system to enable the collection and analysis of financial crime data across multiple law enforcement authorities.

In 2019/2020 an additional £1.5 million of government funding was allocated to the ECU including £707,000 for the procurement of a new IT system to enable digital searching of information and funding for new posts, including the appointment of a forensic accountant. Almost £400,000 of extra resources was allocated for the ITD and Customs Divisions to strengthen their international compliance teams. The FIU was allocated an additional £93,000 to help improve the depth and scale of investigations, the ICART received an additional £297,000 to establish the unit on a permanent basis and the GSC received £145,000 to ensure it retains the necessary expertise to continue to develop appropriate regulation and ensure compliance.

The national framework for combatting ML was re-assessed for this NRA using the framework of the World Bank model. The authorities considered and contributed to a full review of the national framework and have provided supporting evidence for the assessment. Every area assessed either maintained or showed improvement from 2015. The conclusions reached reflect the progress that has been achieved from addressing to date over 90% of the recommended effectiveness actions made in the MER. Actions taken have been reported upon in detail to MONEYVAL by the IoM in 2018 and 2019 and progress continues to be reviewed.

4. Main Threats – Money Laundering

This section of the report considers the domestic and international threat of ML to the IoM. This threat derives from predicate offences being committed in the IoM which create the proceeds of crime and also predicate offences committed outside of the IoM, with criminals attempting to move the proceeds of crime into or through the IoM to other destinations. The nature and volume of the predicate offences in each case is different. The international threat is significantly higher in terms of the amount of proceeds concerned.

Overview of International Threats

The methods employed in generating international proceeds are varied and often complex and sophisticated in nature. The economy of the IoM has significantly diversified in recent years into non-financial sectors; e-Gaming, which is inherently international in nature, is currently the largest sector for the IoM and Information and Communication Technology (ICT) services also have a significant presence. Financial and other business services continue to make up around 31.5% of national income[15]. The largest financial sector in the IoM is insurance, with life insurance forming the largest part of that sector, followed by banking.

Cross-border banking business for the IoM currently represents around 0.15% of global cross border business; 34% of customer deposits are domestic, 30% from the UK, 8% European (Including the EU) and 28% other[16]. Although the IoM is not a major international banking centre the services provided presents the potential for illicit funds to enter and move through the IoM, in particular as part of a process to disguise the origins of the proceeds. Moreover the multiplicity of channels and methods available to sophisticated criminals, including organised crime groups, present ongoing challenges.

In respect of assessing the overall level of threat, the IoM now has access to much fuller data than when the NRA was first conducted. The data shows that 98% of all inflows and 96% of all outflows are to or from jurisdictions of lower or at least equivalent level of risk to the UK, which is the largest trading partner of the IoM. Less than 0.5% of inflows and outflows are from/to the highest risk countries. The origin and destination of financial flows is dealt with in the chapters on TF and the section on Banking and elsewhere in reference to the activities of particular sectors.

The IoM is an international finance centre; the main threats to the IoM arise from international ML where the proceeds are derived from foreign predicate offences, using the wide range of financial and non-financial services available. The types of services provided in the IoM, although generic in nature, are nevertheless attractive to criminals and may be used to conceal the proceeds of crime or as part of a process to disguise the origins of those proceeds through international transfers of funds and the use of complex corporate structures. Chapter 8 looks at the types of legal structures available in the IoM; Chapter 7 considers the risks around professional intermediaries and Trust and Corporate Services Providers. A further risk is where criminals may seek to use jurisdictions such as the IoM, which has a stable government and established rule of law, in order to protect their assets.

The majority of foreign predicate offences relate to the UK, which is to be expected given the very close economic and geographical links between the IoM and the UK. The majority of International Letters of Request (ILORs) are received from the UK. ILOR data from information collected and analysed by the FIU suggests that there is no other single country or region which presents a

[15] Economic figures 2017/18.

[16] These figures exclude deposits from banks and are based on locational statistics provided by banks to the IOMFSA for the purpose of the IOM reporting to the Bank for International Statistics (BIS).

significantly higher level of risk to the IoM in respect of generating proceeds of crime. Figure 3 below shows the countries from which the IoM has received requests for assistance for the years 2017 and 2018.

Figure 3: Incoming International Letters of Request 2017-2018

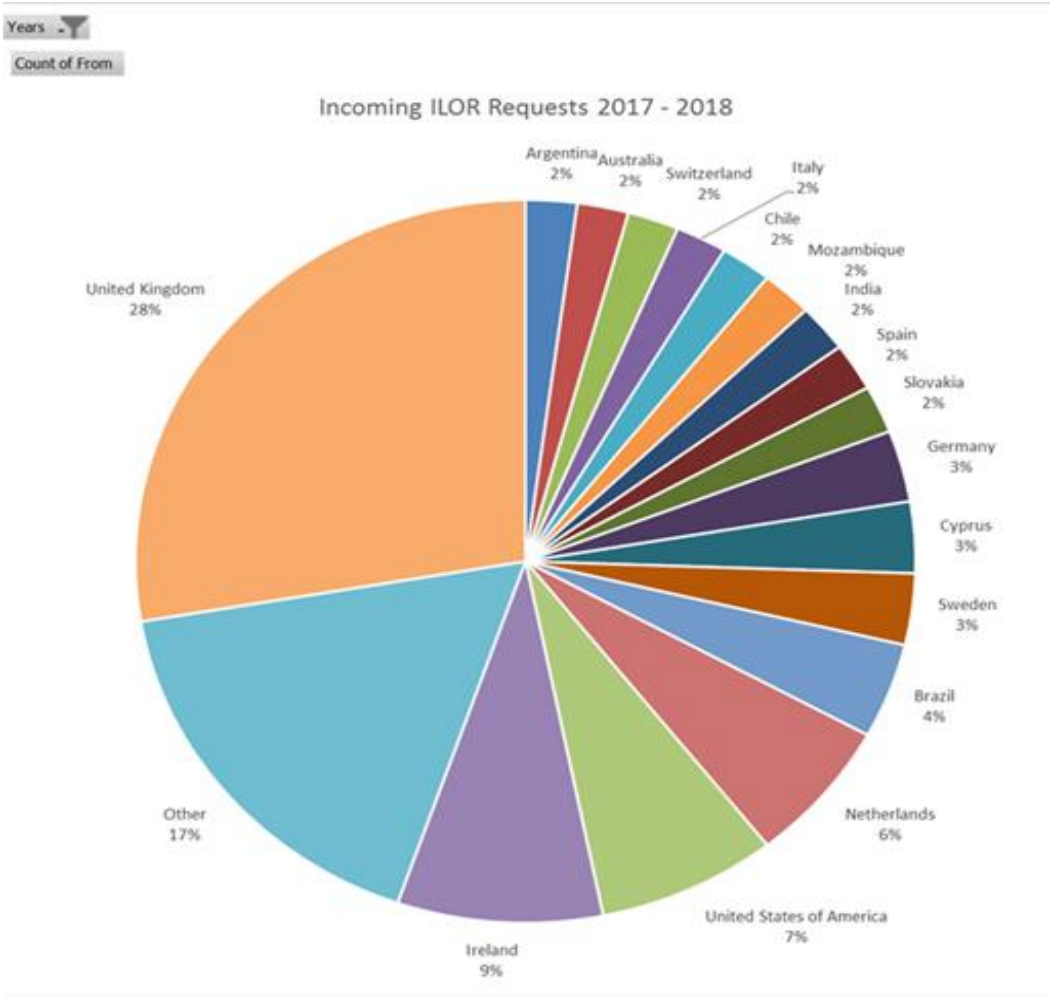
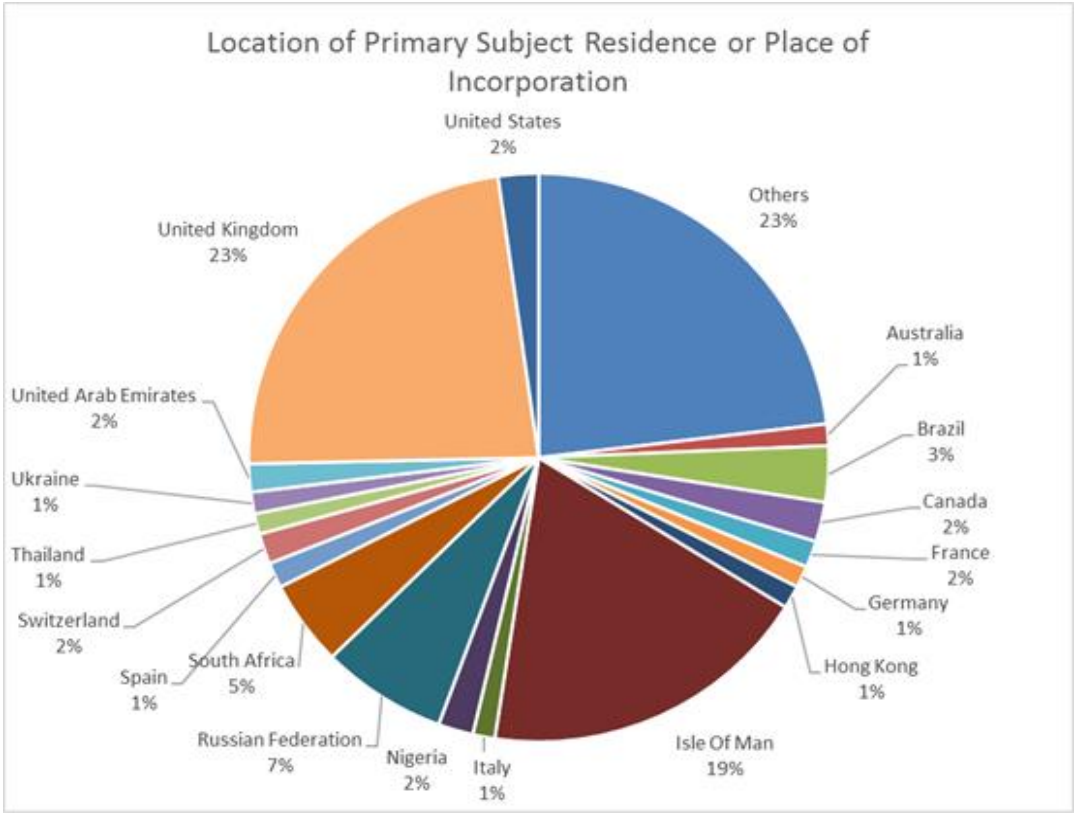


Figure 4 identifies the top 18 jurisdictions in which the subject of SARs received by the FIU were either resident or incorporated.

Figure 4: Location of Primary Subject Residence or Place of Incorporation 2017-18



The main predicate crimes which have been identified as presenting international threats to the IoM are:

- Fraud
- Theft
- Corruption and bribery
- Tax crime
- Drug Trafficking

There are a number of other areas which are emerging as risk, which the IoM authorities are aware of, including:

- Cybercrime
- Human trafficking and slavery

Figure 5 shows the % of SARs submitted by sectors in 2017-18. In comparison to 2013 data provided in the previous NRA, overall reporting by banks has decreased as a proportion of the whole from 66% to 54%, as has TCSP reporting from 14% to 9%. This can be accounted for by the significant increase in reporting by online/e-gaming, from 6% in 2013 to 18% last year. The sophisticated systems in use by online gambling companies are adept at identifying suspicious transactions, e.g. credit card frauds, which are reported to the FIU. The FIU has reported a drop in overall volume of SARs by 10% on the previous year, which is considered to be a result of improved engagement with industry, resulting in fewer but better quality SARs, demonstrated by an increase in the number of intelligence packages being disseminated to local law enforcement.

Figure 5: Originator Sector Breakdown of Suspicious Activity Reports Received by the FIU – 2017/18

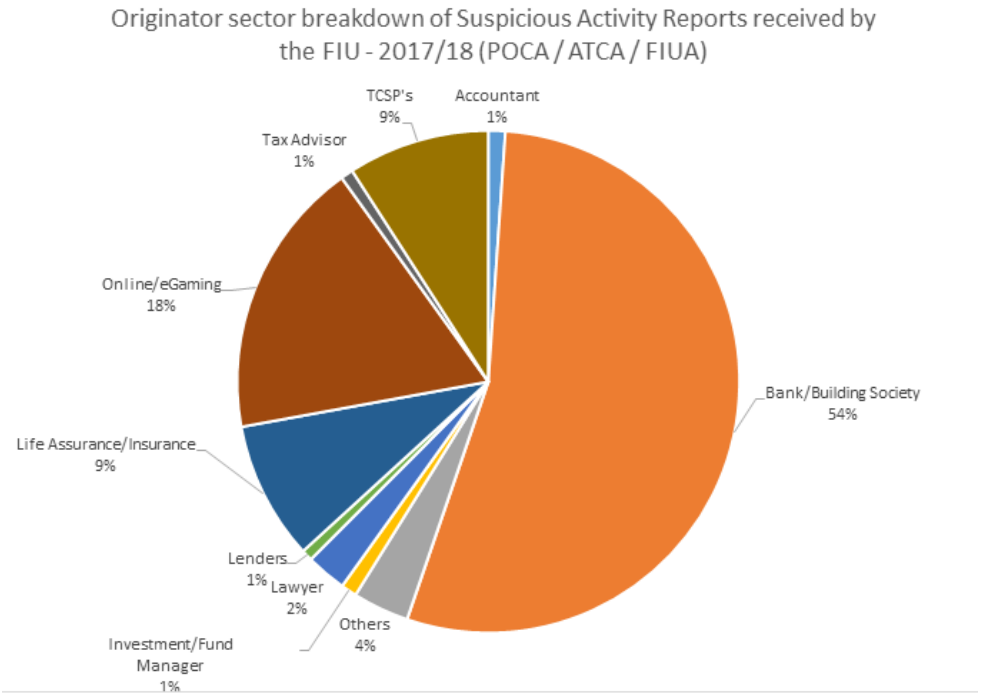


Figure 6 illustrates the % of SARs by suspected criminality received by the FIU; 'money laundering' is often the identified criminality where the underlying predicate offence cannot be determined. Table 3 provides figures concerning investigations completed by the ECU in 2018-19.

Whilst the FIU figures identify tax evasion as the suspected criminality in 29% of cases, relatively few tax cases are investigated by the ECU (although those that are can be extremely large cases). The reasons for proportionally few tax cases being investigated by the ECU are explained elsewhere in the NRA.

Figure 6: % of SARs by Suspected Criminality 2017-18

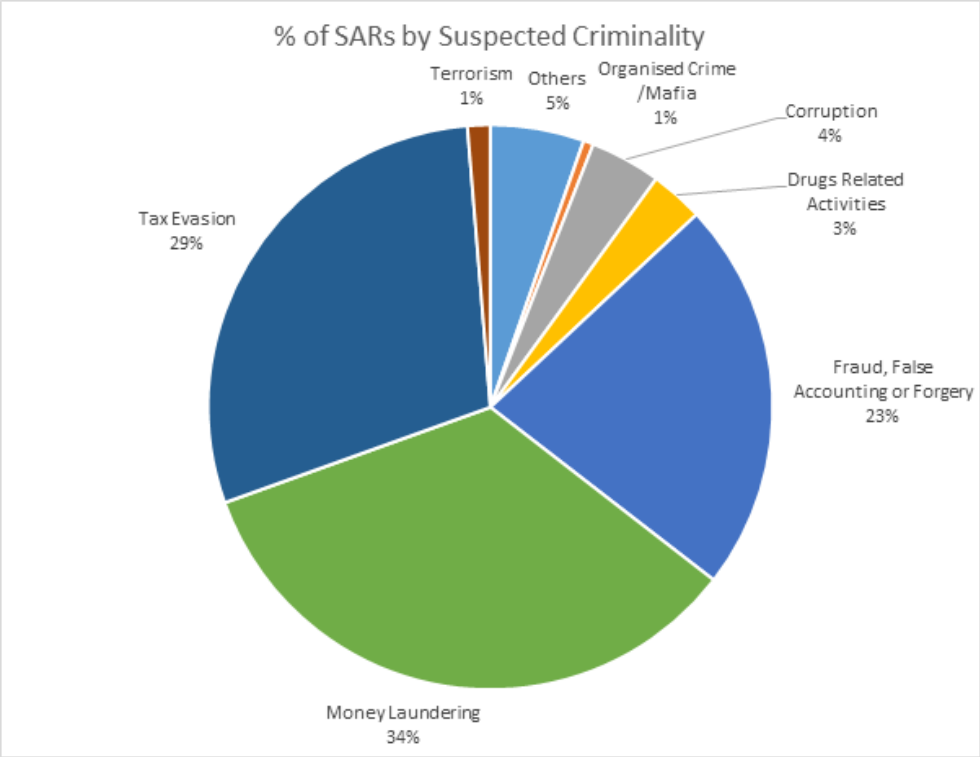


Figure 7 below shows the nature of the predicate offences identified in international requests received in 2017 and 2018. Where ML is identified, this is because no specific predicate has been included. Request for international assistance in respect of tax are sent directly to the IoM tax authorities and therefore are not included below. Data concerning the country of origin of tax requests is confidential under international agreements.

Figure 7: % of ILORs by Predicate Offence 2017-18

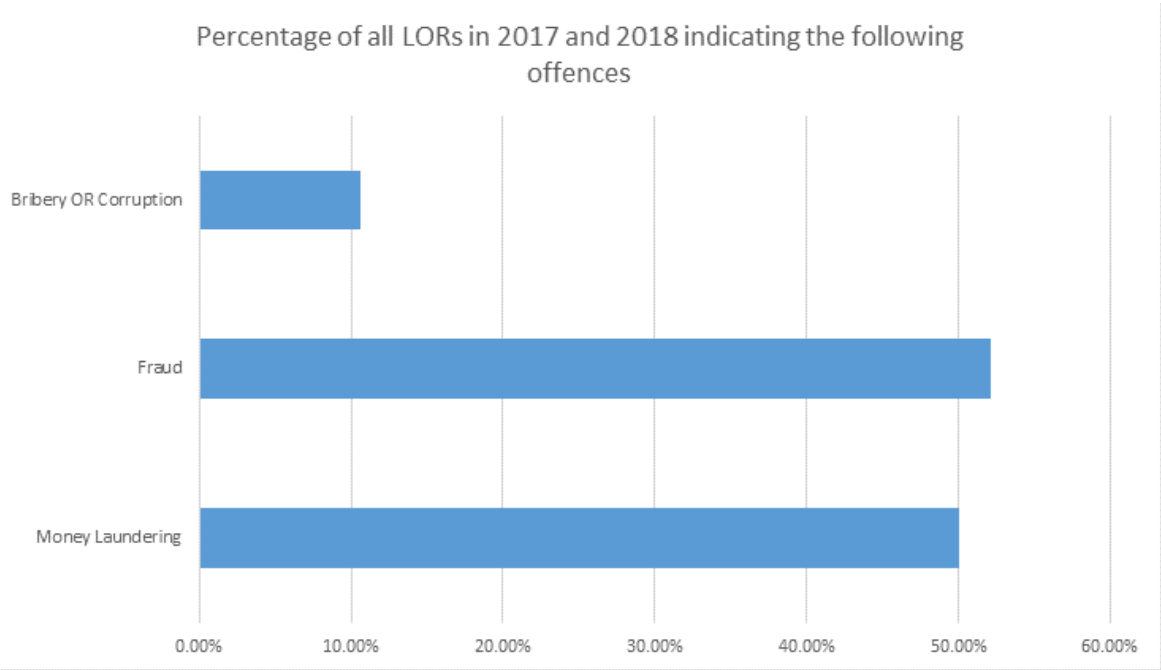


Table 3: Investigations completed by the ECU in 2018/19 by predicate offence.

Predicate Offence	No. of Investigations	Percentage of total	Domestic	International
Fraud	10	27%	4	6
Corruption and Bribery	7	19%	1	6
Robbery or Theft	5	14%	3	2
Tax Crimes	4	11%	1	3
Unknown	4	11%	2	2
Terrorism inc. TF	2	6%	1	1
Drug Offences	1	3%	0	1
Forgery	1	3%	0	1
Insider trading and market manipulation	1	3%	0	1
Other	1	3%	0	1

The table below shows the number of ML investigations undertaken by both the ECU and the wider IOMC. The seizure of funds domestically and investigation and prosecutions of crime by the IOMC is predominantly linked to the supply of drugs domestically.

Table 4: Money laundering investigations completed in 2018/19

	No. of Investigations.	Domestic	International
Completed by ECU	10	4	6
Completed by IOMC	27	27	-

During 2018/19 the ECU adopted 13 new ML cases of which 6 were domestic and 7 were international; by the end of 2018/19 the ECU had a total of 32 investigations ongoing of which a number were ML investigations.

Fraud and Theft

The identified offences known or suspected of generating the most significant proceeds of crime in the IoM are fraud and theft. 23% of SARs submitted in 2017/18 concerned fraud or related matters and fraud and theft accounted for 41% of the investigations completed by the ECU in 2018/19.

Crimes are frequently computer-enabled with electronic payments enabling money to be moved quickly from one account to another with the IoM at risk of being used as a conduit through which to channel proceeds onto other destinations. Recent analysis by the National Fraud Intelligence Bureau of the City of London Police identifies a growing number of financial investment frauds linked to Crypto currency investments with Initial Coin Offerings (ICOs) and Crypto mining emerging as new methods of fraudulent investments. There is also evidence of money obtained through fraudulent schemes being converted into Crypto. While there have been no identified cases in the IoM to date this typology presents a clear threat.

Because of the international nature of business conducted in the IoM the predicate offences which generate the largest proceeds of crime are often committed elsewhere and the criminals involved in ML may not be present in the Island. However IoM residents have occasionally been identified as being involved in directing or facilitating 'high-end' international ML. Equally even

with predicate offences outside the IoM, the ECU still has a high percentage of suspects who either partially or fully reside within the IoM and are suspects within current investigations. Of the current live cases 15 suspects are attributed to the IoM.

Case Study

In 2018 an individual in the IoM was successfully prosecuted for attempting to launder the proceeds of a fraud committed in France. The Defendant was indicted with laundering over €300,000 from thefts of credit balances in France receiving it into an account in the IoM and then attempting to transfer it to an account in Asia. There was no prosecution in France for the predicate thefts; however this did not prevent a prosecution for money laundering of the funds within the IoM.

The ECU and the Prosecutors proved that the money was criminal property, evidencing that it was not acquired legitimately by the Defendant for services rendered to the Company. The funds were intercepted and repatriated to France. The defendant was convicted and sentenced to 3years and 2 months in custody.

Corruption and Bribery

Whilst crimes of deception (fraud and theft) are noted as the largest threats in relation to generating proceeds of crime, other predicate offences have been recorded; these include bribery and corruption. In 2018/19 19% of matters investigated by the ECU concerned bribery and corruption. The threat arises substantially from those seeking to launder proceeds of these offences through the IoM rather than from domestic predicate offences. This might be in a number of ways including using companies or other legal arrangements to purchase land, property or other assets. It is therefore essential for industry to identify and verify politically exposed persons (PEPs) including their close associates and family members when taking on customers. There are also additional requirements under the AML/CFT Code for PEPs including establishing the source of wealth and undertaking enhanced monitoring.

As an IFC, businesses in the IoM have customers who are not resident and whom they deal with non-face to face; these customers may have been introduced by a third party and may be High Net Worth Individuals (HNWI). Although these are familiar and unexceptional features of IFCs, the NRA highlights the importance of clearly identifying the underlying customer using information which is verified by the IoM entity in order to manage and reduce risk. MONEYVAL made a number of recommendations regarding use of intermediaries / introducers and evidence of identity. New legal requirements have been introduced and the regulators will now need to ensure that these are being implemented effectively by industry.

Ownership of property by foreign companies, especially high-end property in the UK, has come under intense scrutiny in recent years as concerns have grown that property and land are highly attractive assets for the proceeds of foreign corruption in particular. Ownership of multiple and/or expensive properties through complex structures, sometimes involving several jurisdictions, is a recognised ML threat. Often the true beneficial owner and the source of wealth used to secure property can be difficult to identify.

In 2018 it was estimated that trusts and companies established in the IoM owned around 12% of the UK properties[17] owned by non-UK companies. There are practical and legitimate reasons why property might be held through IoM structures; to date very few SARs have been received that relate to property and it has not been an area where requests for international assistance have been received. Nevertheless those involved in establishing or operating trusts and companies which hold such assets need to ensure that they are aware of high risk indicators.

Yachts and aircraft (private and corporate jets) are not identified as a significant ML or TF risk for the IoM. Yachts and aircraft are attractive assets for HNWIs and ownership may be either direct or via managed companies in the IoM. Where crafts are managed by IoM companies the local CSP carries out full CDD checks on their customers including beneficial ownership and identification of PEPs, as prescribed by the AML/CFT Code.

The IoM has a Ship Registry and a separate Aircraft Registry. Both Registries carry out further checks on their customers to mitigate the risk. Legally binding and admissible Declarations are required by the Aircraft Registry and those details must be kept updated by industry.

There is however always a residual chance that such high value assets may be purchased using the proceeds of crime and corruption. When taking on new business both Registries check the sanctions listings, review open source material and undertake searches using Worldcheck; the FIU is also requested to undertake background checks should suspicions be raised. If any links are found to criminality then applications are refused. There is close cooperation between the IoM Ship and Aircraft Registry and with their respective international agencies and both work closely with CED.

The Ship Registry requires all vessels over 24 metres to have transponders fitted. The Aircraft Registry focusses on business jets above a certain size. It also has wide powers under Article 4 of the Air Navigation (Isle of Man) Order 2015 which states that any aircraft must not be registered, or allowed to continue to be registered, if it is deemed not to be in the public interest. Aircraft will be de-registered if there are reasonable grounds to do so[18].

The 2017 Serious and Organised Crime Threat Assessment[19] flags sports corruption as a threat. Sports corruption is relevant to the IoM as the GSC has licenced operators offering online sports betting across a wide international spectrum which provides significant opportunities for fraud and corruption. The GSC has established MOUs with various anti-sports corruption entities, who can contact the GSC with any concerns regarding suspicious sporting events and betting patterns connected to it. The GSC then liaises with the licence holders with a request to respond with relevant any information. Information is then relayed back to the anti-sports corruption entities which will then review it and decide on any further actions.

Tax Crimes

- Direct taxes

The Isle of Man's income tax rates include a standard zero rate for companies, as well as other rates of tax which may appear to be attractive to persons living outside the Island, who may see them as an opportunity to invest in the Island in order to reduce their liability to tax, or shift

[17]BBC analysis, February 2018
[18] The power to de-register aircraft has been applied in 2019
[19] Europol 2017

profits from, their home country. This is a risk both in terms of receipts through tax evasion or avoidance; and to the Isle of Man's reputation on the international stage.

In the IoM in 2017/18 29.2% of all SARs submitted to the FIU concerned tax matters. 38.5% of the SARs submitted by banks/building societies and 50.4% by TCSPs related to suspected tax evasion and 11% of the matters investigated by the ECU in 2018/19 concerned tax crimes.

Investigating the predicate offence of tax evasion is challenging since there is a very inconsistent approach internationally to cooperation in sharing intelligence and working cooperatively on suspected tax offence matters. The ECU works closely with the other domestic law enforcement authorities (LEAs); a tasking process ensures that suspicious activity reports (SARs) concerning tax are brought to the attention of the most relevant authority both internationally and domestically. The ECU adopts a criminal investigation only where a high level threshold is met. As such the numbers of ongoing investigations for tax evasion represent around 10% of the current workload. It should be noted however that the longest standing criminal investigation taking place is based around tax evasion offences.

A significant percentage of the incoming international requests for tax information that are received by ITD concern individuals. These may be straightforward matters where the individual has a bank account or insurance products set up in their own name or they may be where the individual is identified as a beneficial owner of an IoM company, a trust or as a participator in a scheme; requests are also received concerning legal persons, for example IoM companies liable to tax in other jurisdictions.

In order to mitigate risks around tax evasion the Isle of Man Government has implemented a number of global tax measures aimed at improving transparency. These measures include implementation of the OECD Global Forum's international standard on Transparency and Exchange of Information for Tax Purposes, and which includes in the latest round of reviews, an assessment of access to, and availability of, beneficial ownership information based on the FATF definition.

Further measures aimed at mitigating risk are detailed in Appendix I.

Case Study

Self-laundering by a Danish individual, involving a complex evasion of Danish corporate tax. Funds held in an IoM bank account in the name of a foreign company of which the individual was found by the Danish Court to be UBO. ICART registered the Confiscation Order made in the Danish Court here in the IoM and enforced it against the funds in the IoM bank account. Useful jurisprudence was created, interpreting the relevant legislation such that it is not necessary to prove precise dual criminality, but a correlation between a foreign offence and one on the IoM statute book.

The MONEYVAL Report of December 2016, included a recommendation that;

"The IoM should continue with its efforts to seek agreement from its international partners to provide information in relation to criminal requests to the FCU on a general basis and in the interim should continue with its current practice of seeking the express written consent of the

treaty partner (TIEA OECD) as required under the confidentiality article of the relevant international agreement in appropriate cases."

While it has not been possible to obtain consent on a general basis, the Assessor of Income Tax[20] is continuing the practice of seeking express written consent in the context of actual requests received, which would allow for information to be given to the FIU in respect of criminal cases. This remains a challenge for the IoM, as some countries have indicated that consent cannot be given and others fail to respond in a timely fashion and only in a small number of cases has consent been received.

- Indirect Taxes

Many of the indirect taxes on the Island correspond to those in force in the United Kingdom, an obligation the Island has through the Customs and Excise Agreement 1979. These include customs and excise duties and Value Added Tax (VAT). Consequently this allows for the general free movement of goods between the IoM and UK (with some exceptions for prohibited and restricted items), and while the UK remains part of the EU, goods are able to freely travel within the EU also.

Due to its geographical location, there are few direct imports into or exports from the Island and certainly there is no evidence or intelligence that suggests the IoM is being used to introduce goods into the domestic or EU markets which have not been subject to the appropriate duties. However, there is a risk that legal entities on the IoM could be used in supply chains with the aim of circumventing customs duties elsewhere. The IoM has co-operation mechanisms with the UK, EU member states and customs authorities around the world which enable the sharing of information in order to identify and prevent such crime. Since 2016 CED have received 108 mutual assistance requests, mainly from the UK and EU member states, and have sent 3 to other customs authorities.

Drug Trafficking

Drugs trafficking is one of the most significant contributors to illicit proceeds worldwide; it impacts all types of communities whether large or small, urban or rural and the IoM is no exception. The impact of drugs, drug dealing and the proceeds of that crime are experienced in a very direct way via the importation of drugs predominantly from the North West of England and the involvement of organised crime gangs. This area is dealt with under domestic threats later in this section.

The international threat concerns the laundering of the proceeds of drug dealing through integration and layering of those proceeds using legal vehicles such as companies and trusts with deliberate efforts to increase complexity in order to disguise the beneficiaries and the source of the funds. Whilst the IoM Constabulary (IOMC) deals robustly with domestic drug offences, there are relatively few investigations concerning the laundering of funds linked to drugs crime. Evidence suggests that ML risks through the IoM are not necessarily driven by drugs trafficking as seen within other illicit proceeds worldwide.

[20] Who is the Competent Authority for all of the Isle of Man's international tax arrangements

Cybercrime

Cybercrime is a relatively new and evolving area where regulation is currently struggling to keep pace. The adaptation of technology doesn't create new crimes, but provides new platforms for enabling crimes such as fraud, theft and blackmail to be conducted in new ways and with greater speed, efficiency and anonymity. The broad international reach and the speed with which cybercrime can be committed make it hard to address. Even identifying that a crime has taken place can be difficult and the levels of encryption and lack of a 'footprint' can make investigation challenging. Victims may be global and numerous and so reparation also becomes an issue. Increased specialist resources, time and technical expertise is therefore required in order to effectively investigate such cases. It is notable that a number of investigations that the ECU is dealing with have a strong technological element to them.

The IoM Constabulary has produced a cybercrime strategy which aims to develop the IOMC and its workforce to meet the operational threats and to seek innovative ways to build 'Prevention' as a key thread of the strategy. The strategy also aims to strengthen collaboration, in particular with the IoM Government Office of Cyber Security and Information Assurance, around prevention and collaboration with UK counterparts within the National Cyber Security Centre. The latter will provide a pivotal route for operational support where necessary. These links have begun and support received in 2019 with ongoing criminal cases regarding significant Distributed Denial of Service (DDoS) and Ransomware attacks against IoM Institutions.

Human Trafficking and Slavery

The FATF identifies human trafficking as a predicate crime and currently it is estimated that there are around 40 million slaves worldwide. After drugs and counterfeiting, human trafficking/slavery is thought to be the third largest crime worldwide. In 2014 the International Labour Organisation estimated that $150 billion is generated annually through forced labour.

To date the IoM has received a small number of SARs in 2017/18 raising suspicions of funds in the IoM connected to human trafficking and a few requests over the same time period for information from industry connected to suspected human trafficking in the UK. The financial flow data shows that 2% of inflows and 4% of outflows are to higher risk jurisdictions (with less than 0.5% of total inflows and outflows being from/to the *highest risk*) including some countries where it has been identified that cash generated from human trafficking and smuggling is sent to following integration into the financial system.

More detailed analysis is required (as part of the overall risk based approach to supervision) to ensure that the nature and origins of these financial flows is understood. No requests for mutual legal assistance in connection with human trafficking and slavery have been received, or issued.

The Panama and Paradise Papers

As a result of the publication of information contained within the Panama and later the Paradise Papers, (both posted by the International Consortium of Journalists), the FIU conducted an intelligence review. The Panama Papers generated the greater number of new disclosures from the IoM regulated sector (72), or referred to matters with a connection to information already held by the FIU. As a result of the disclosures received, 100 disseminations were made to domestic and international law enforcement agencies (LEAs) and FIUs. In two cases, dissemination of intelligence to domestic LEAs which originated from disclosures received from the regulated sector and which had a connection to subjects referred to in the Panama Papers, resulted in IoM assets being restrained under the Proceeds of Crime Act (POCA) 2008.

The UK accounted for the highest number of disclosures received and disseminations. Domestic disseminations were mainly to the IOMFSA. This was in line with the non-criminal nature of most of the information made public in the Panama Papers.

Although disseminations were made to international LEAs and FIUs in all appropriate matters, there were no international letters of request for mutual legal assistance received which were attributable to disseminations related to the Panama Papers, nor any requests in respect of matters not known to the FIU before the publication of the Papers. Due to the lack of feedback received it is not possible to analyse the reason for this, but one explanation may be that the receiving jurisdictions took the view that the activities highlighted in the Papers were not criminal in nature. Mutual legal assistance is available only where a criminal investigation or prosecution is underway.

The FIU received 15 disclosures from the IoM regulated sector in relation to the Paradise Papers. 26 disseminations were made to domestic and international law enforcement agencies, including regulators, and FIUs. The relevant intelligence was received and disseminated in line with usual best practice and the FIU established an Operation to ensure that there was an awareness of the links between the matters and analysis carried out in light of those links. In this way, the relevant matters were dealt with so as to ensure comprehensive and fully analysed intelligence packages for LEAs and FIUs. Furthermore, the FIU was able to monitor the overall impact of the publication.

The impact was in fact limited. Many of the issues raised by the Paradise Papers relate to financial practices which, whilst engaging media and the public interest, were not illegal. The relatively low number of connected disclosures which were made following publication makes sense when viewed in that context.

Overview of Domestic Threats

Fraud, Forgery and False Accounting

Illegal proceeds generated within the IoM are substantially driven by fraud, false accounting and forgery. In 2018 the FIU received a total of 433 disclosures where the criminality, or suspected criminality, was fraud, false accounting or forgery. In 71 cases, the IoM was the country of residence or place of incorporation of the main suspect. In line with overall figures, the banking sector is the most frequent reporter of fraud, false accounting and forgery, and reported 44 (62%) of these 71 disclosures. Common examples of the activities amounting to fraud, false accounting

and forgery in both domestic and international reporting, are Ponzi schemes, credit card fraud and (in the majority of domestic cases) benefit fraud.

Whilst fraud as an offence has seen an increase recently this may be partly as a result of the preventive measures introduced by banks working with IoM law enforcement (the Preventative Banking Protocol) aimed in particular at protecting vulnerable customers. In 2019 the Protocol prevented more than half a million pounds of residents' savings being lost to online investment and romance frauds.

Direct Taxes

Drugs, domestic tax evasion, theft and burglary also create proceeds of crime, but on a smaller scale. In 2018, the FIU received 34 disclosures (equating to 1.9% of all disclosures) relating to suspected tax evasion with an IoM resident or incorporated subject. Most of the disclosures (64.7%) were from the banking sector, followed by Lawyers (11.8%). Prominent grounds for suspicion were activity on an account that was not in keeping with expectations, and suspicious cash transactions, for example, transferring cash in tranches to circumvent reporting obligations in another jurisdiction.

A random sample of 20% of the disclosures relating to tax evasion indicated low value offending. The 34 disclosures that referred to domestic tax offences whereby the IoM individual or company were suspected of evading IoM taxes 23 (67.6%) related to IoM individuals only, the remaining 11 were concerning mostly small IoM companies / sole traders and 4 matters where the IoM company was suspected of VAT offences.

Data on tax non-compliance over a number of years indicates relatively little change. In 2017/18 a total of 633 tax cases were started by ITD and fines of £50,978 imposed; this is a rise from the 2015 NRA, which were 558 tax cases in 2013/14 and fines of £32,175. A large proportion of ITD work is focussed on international matters, which is addressed in more detail above.

Indirect Taxes

Value Added Tax fraud also presents risks. Legitimate trading companies may be exposed to ML risks from purchasers of the goods or services that a trading company is selling. Because of the identified risk from missing trader intra-community fraud (MTIC)[21] it is the policy of CED for law enforcement officers to examine all new VAT applications. Between January 2016 and August 2019, 20 legal entities were refused permission to register for VAT because of the suspicion of involvement with fraudulent supply chains. CED also review all requests for mutual assistance for possible offences of ML/TF. The cases dealt with by CED are low in number; there is no evidence that one type of company structure is more vulnerable to VAT fraud than any other.

With the high cost of moving goods on and off the Island and the fact that duty rates are in line with the UK there is no evidence or intelligence that suggests the Island is used for diversion of goods normally liable to excise duties or laundered fuel that has had the red marker removed.

Drug Trafficking

Drug trafficking and selling of drugs are proportionately significant domestic predicate crimes in the IoM. Drugs are brought into the IoM predominantly from the NW of England to be sold in the Island. This is a well-established pattern of criminality, which is reported upon annually by the

[21] Also known as 'carousel fraud' because of the way that the goods keep moving around without ever reaching a final consumer.

IoM Constabulary. Criminals then look to export the cash proceeds into the UK where integration of the funds is easier than in the smaller and highly formalised economy of the IoM. The IoM Constabulary has reported upon the involvement of UK organised crime groups in this trafficking.

Drugs account for the main cash-based criminal activity in the IoM. In 2016-17 drugs with a street value of £781,863 were seized; in 2017-2018 seizures rose to £883,868.[22] Suspicions related to the trafficking and selling of drugs are generally not reported upon via the FIU, possibly because domestic drugs proceeds do not go through the finance sector. It is important to ensure that where these proceeds may enter the IoM finance sector that industry can identify them and report accordingly.

Implications and Conclusions of the Threat Assessment for Money Laundering

The role of the "gatekeeper" institutions in the IoM, lawyers, accountants and the TCSP industry generally, will continue to be critical in helping to address fraud, theft, tax evasion and other such crimes. In this respect, the work undertaken by the FIU on SAR reporting and the supervisory role of the IOMFSA and the GSC will provide support and assistance. Internationally, whilst extensive global measures have been introduced to try and tackle the challenge of tax evasion, this is likely to continue to be an important predicate offence for the IoM. This is recognised by ITD who continue to prioritise international cooperation to address this challenge and that of tax avoidance.

The growth in cybercrime, for example crimes committed using ICT technology and crimes such as fraud, the scale of which can be significantly magnified by the use of ICT, is now a dominant threat and one which only specialist knowledge, skills and resources and strong partnership working can seek to address. This is recognised and the IoM has a separate and detailed cybercrime strategy which is managed and delivered by leads within the Economic Crime Unit. Domestically fraud and the growth in targeting the IoM for supplying illegal drugs will present a continuing challenge to identify and seize the proceeds and instrumentalities of increasingly professional criminal gangs.

The prevalent typologies are well-recognised and there are measures in place aimed at preventing the abuse of financial and non-financial services. The exposure of the IoM to higher risk jurisdictions is relatively low although further analysis work is required in respect of both financial flows and the annual data returns now provided to the IOMFSA by regulated entities and DNFBPs. Emerging threats from gambling and ICT need to be carefully monitored as these continue to develop and expand. The information available supports the findings of the 2015 NRA and the ML risk to the IoM is assessed as **Medium High.**

[22] Chief Constables Annual Report 2018-2019

5. Main Threats - Terrorist Financing Threats

Overview

The 2015 NRA assessed TF risk in the IoM as Medium Low; the risk of actual terrorist activity was and is considered to be Low. TF in the IoM could potentially present itself as self-funded or raising funds domestically for onward transmission or the use of sophisticated and complex international structures to disguise the origin and destination of funds intended to support terrorist activities. The latter is considered to present the more evident risk.

The risk of domestic TF for the IoM is considered less relevant than that of international financing for terrorism using company structures including potentially non-domestic charities and other NGOs. The potential raising of funds for travel, training, promotion or other support for terrorism from the IoM should not be ignored, but is considered to be less of a threat. During the relevant period, no letters of request for mutual legal assistance were received (or issued) relating to TF.

The relevant geographic and demographic factors, the available intelligence and low levels of TF SAR reporting, requests for MLA etc. indicate that domestically the IoM has a Low risk for TF; nevertheless the IoM has direct links with, and is closely situated to, the Republic of Ireland, Northern Ireland and to the mainland UK. It is therefore important to keep aware that any changes in the security situation in those jurisdictions may have an impact on the Island, whether in respect of traditional models of TF, or TF funded via organised crime from groups external to the IoM.

Cross-border TF threat for IFCs

The IoM has contributed to a MONEYVAL guidance-paper on TF threats and vulnerabilities in IFCs; the paper has provided guidance on TF risk for this NRA and is also referenced in a FATF report 'Terrorist Financing Risk Assessment Guidance' 2019. The MONEYVAL guidance was prepared on the basis that the primary TF risk for most IFCs is likely to arise from their use as transit jurisdictions for the movement of funds linked to terrorist activity outside the jurisdiction, or from their involvement in the management of foreign funds or businesses that are linked to such activity.

The guidance-paper identifies two aspects for the assessment of the TF threat of an IFC. The first is to look at connections between the IFC and a target jurisdiction, including the extent to which the IFC's businesses or NPOs may be involved in the international movement of goods that could be used for terrorism or to finance terrorist activities. The second is to consider the extent to which terrorism or TF is occurring in jurisdictions with which the IFC has close geographical and/or political links.

The assessment of vulnerability for IFCs requires an examination of the extent to which the services or products offered by IFCs are likely to be attractive for TF purposes; and the extent to which the IFC has adequate measures in place to address TF.

The measures available in the IoM to address TF (and PF) are outlined below; consideration of products and services attractive to TF and the controls around those can be found in the relevant FI and DNFBP section.

Financial Flows and other data

The 2016 MONEYVAL assessment recommended that the IoM authorities should seek clearer evidence to support an assessment of Medium Low risk for TF, notably data from IoM banks

concerning the origin and destination of financial flows, and also recommended that a detailed review was undertaken of the few TF SARs available.

The financial flows presented a challenge as there is no central bank for the IoM; the IOMFSA has therefore undertaken detailed work with banking groups in the IoM (most of which are part of wider international groups) and now receives inflow and outflow data on a quarterly basis. This data is also shared with the FIU for analysis.

The data shows that in 2018 2% of all inflows and 4% of outflows were connected to higher risk jurisdictions[23]. However, only 0.32% of all inflows and 0.44% of all outflows were from / to the 29 highest risk countries.

Further work is required to analyse inflows and outflows in more detail to better understand the nature of the transactions for TF and ML risk given that a number of these countries are jurisdictions which have, for example, been identified as at risk from receiving cash generated from human trafficking and smuggling after integration into the financial system.

The FIU has also analysed data in respect of 20 jurisdictions deemed to have a high TF risk in relation to the IoM, which shows that between April 2016 and May 2018 around 4.5% of disclosures to the FIU had links to a number of higher risk jurisdictions.

From 2017 to 2019 the ECU investigated 15 TF cases. Of those 15 cases only one developed into a credible criminal investigation; this case ultimately resulted in no further action being taken as there was a lack of evidence to support any criminal charges. All other cases were concluded through mitigation measures including liaison with reporting institutions. In a number of cases, it was identified that the suspicion was not TF related although it had been reported as a SAR under ATCA legislation.

Overall assessment of the cases investigated has not identified any specific typology, but there is a higher concentration of referrals from the gaming sector, usually referring to the use of pre-paid cards or multiple use accounts. The data set is still too small to enable any meaningful assessment or conclusions. It is apparent that the level of awareness of TF within industry generally has increased, which is leading to more disclosures. This is also the case within law enforcement and the assessment and supervision of TF matters within the ECU.

The IOMC, which is the lead agency for the national TF Strategy, undertook a review of TF referrals in 2018 along with other LEA key stakeholders. The review did not identify any specific typologies or new risks but areas for strengthening the TF Strategy and the underpinning operational processes were identified.

The IOMFSA has also undertaken a review of the level of use of the IoM by charities/NPOs which are not registered in the IoM (foreign NPOs). The risk of foreign NPOs using IoM structures to fund TF was an area identified during the MONEYVAL assessment in 2016. At the end of December 2017 the total number of foreign charities/NPOs reported by banks was 14. During 2017 IoM banks accepted one new foreign charity/NPO and no applications were declined or terminated for ML/TF reasons.

[23] For the purposes of this report, higher risk jurisdictions (including those considered the *highest risk*) are those jurisdictions identified by the IOMFSA, that may posing a higher risk of ML/TF via the FATF lists and a composite rating derived from the higher of the Aon Risk Index scores and the Basel AML/CFT index.

Preventive Measures

There is little evidence that the products and services available from the IoM are uniquely attractive or in some cases e.g. domestic NPOs, amenable for TF. Whilst there is a lack of typologies domestically and globally of the use of trusts and company structures for TF, however this does not mean that there is no risk. Larger and more sophisticated terrorist organisations which receive significant donations and/or extort funds from regions under their control will require access to the financial system to integrate, secure and move these funds for TF purposes. Therefore it is important that IoM banks, investments, TCSPs and professional intermediaries are aware of the risks and that there is a high level of collaboration between the authorities and industry to identify and frustrate such activity.

Preventive measures in place include:

- A Combatting the Financing of Terrorism (CFT) Strategy which was adopted in 2018;
- A revised approach to scoping TF risk ensuring that all relevant parties are briefed; a reporting pathway for TF is in place;
- Procedures for the FIU and the ECU for investigating suspicions of TF;
- Close working relationship with UK NW Counter Terrorism Unit;
- ECU Peer review work with UK TF investigations ongoing in 2019;
- Close working relationship with the UK NCA Regional Organised Crime Unit and ongoing work to reinforce MOUs;
- The competent authorities ensuring that relevant information and advice is disseminated internally and to industry and provide focussed training events on TF and TFS for industry;
- Typologies provided by the FIU to industry and to the regulators in respect of TF;
- The production of 'Real Time TF Guidance' for industry explaining what happens to a TF SAR and making recommendations on the practices to be adopted by industry;
- Published guidance on SAR reporting; in 2017 the number of TF disclosures was twice the average of the previous two year period;
- A regulatory strategy in place for the IOMFSA;
- AML/CFT specific information collected by the IOMFSA as part of an annual return from industry providing data on geographical links, level of exposure to PEPs, the activities being undertaken etc.;
- Training by the FIU and the ECU to IOMFSA supervisory staff to enhance understanding of TF and TFS in relation to supervision of FIs and oversight of DNFBPs;
- A regulatory visit programme to DNFBPs including SNPOs which includes separate consideration of TF threats and sanctions regime;
- Officer attendance at specialist courses including, the National Terrorism Financial Investigators course; Counter Terrorism Investigations training; UK National Crime Agency Financial Intelligence Officer courses; and the UK Metropolitan Police Counter Terrorism Command TF training course.

TF Legislative provisions

The IoM legislation is adequate to enforce any sanctions or other restrictions necessary. The Anti-Terrorism and Crime Act (Compliance with International Standards) Order 2017 criminalises the funding of un-prescribed terrorist organisations for legitimate purposes. The Order also creates a separate offence of financing of travel of an individual for the purpose of preparing, planning, or participating in terrorist acts or providing or receiving terrorist training.

All relevant UN and EU sanctions relating to terrorism financing, as well as relevant UK measures, are fully imposed; information and guidance is provided to businesses specifically about TF sanctions and the risk of proliferation funding. The lists of those designated persons, businesses and entities subject to sanctions are maintained so that they match those in the UK.

New Customs legislation in 2018 delegated the FIU as a body to whom suspicion or breaches of financial sanctions should be reported. Reports of frozen assets and suspected breaches of sanctions are being reported to the FIU. This ensures that industry has clarity on where to report suspicions concerning SARs and sanctions matters. The FIU is the "one-stop" reporting centre for industry. Internal guidance has been published by Customs on designating persons in the IoM who have not been listed in the UK.

Implications and Conclusions

The 2015 Medium Low risk rating for TF reflected geographic and demographic factors and the available intelligence, the effectiveness of SAR reporting of TF related activity, adequacy of resources, the effectiveness of international cooperation, and the strong TF legislative framework in place. The low level of TF SARs, the lack of identified cases and the close formal and informal links between the IoM authorities and with their counterparts in the UK were also factors taken into consideration. These factors are still considered to be relevant and the TF risk for the IoM remains **Medium Low.**

Further actions identified from this NRA include:

- The full analysis and understanding of inflows and outflows of funds to higher risk jurisdictions.
- Using the information and data collated from the regulatory annual returns to further inform supervisory work and preventive measures.
- For the authorities to continue to monitor international typologies and domestic indicators ensuring that findings are appropriately disseminated.
- To continue to thoroughly examine any suspected cases of TF using the policies and procedures established.
- To identify ways in which collaboration with industry on identifying and managing TF risk can be further developed.

Once fuller analyses of inflows and outflows of funds to higher risk jurisdictions is undertaken it may then be appropriate to reduce the TF risk for the IoM to Low.

6. Financial Services

- Banking
- Collective Investment Schemes (Funds), Fund Managers and Administrators
- Asset and Investment Management
- Financial Advisory
- Insurance
- Pensions
- Other Financial Institutions

Summary

Insurance and banking are the main financial sectors in the IoM; insurance is the largest sector at 17.6% followed by banking at 6%. Life insurance forms the largest part of insurance business; insurance businesses are part of large multi-national enterprises and the majority of banking groups are from the UK. Both banking and insurance operate to group standards which apply internationally.

Collective Investment Schemes, Fund Managers and Administrators form a smaller part of the IoM financial services sector, contributing around 1% of National Income. The customer base is substantially non-resident. Other financial institutions in the IoM are limited to small numbers consisting of, for example, bureau de change and e-money services.

The IOMFSA is responsible for the regulation and supervision of those FIs undertaking regulated activities in the IoM including deposit taking, investment business, fiduciary services, money transmission services, insurance, pensions and collective investment schemes.

Guidance (including sector guidance) is currently being updated for all financial and non-financial sectors, in consultation with all relevant stakeholders following the adoption of a new AML/CFT Code in 2019.

Banking

The IoM banking sector is a mature sector, which is fully regulated and supervised by the IOMFSA with prudential and conduct supervision in place. All banks are required to have an internal audit function, most are branches or subsidiaries of larger banking groups and are generally subject to wider group consolidated supervision and need to take into account not only local AML/CFT legislation in devising policies and procedures, but also that of their wider groups.

Banks are generally highly compliant in their approach to AML/CFT matters with well-established customer due diligence and other controls. The use of technological solutions to help identify and combat ML/TF is also becoming more prevalent.

Banks in the IoM provide services to local and international personal customers, corporate and business clients (direct and introduced) as well as persons holding funds on behalf of others (e.g. wealth management). The geographical spread of customers by residency, nationality and location of activity is extensive. A wide range of products and services are provided including savings, current accounts, private and premier banking, investments, lending, treasury services and foreign currency accounts. There is therefore a significant cross border aspect to the IoM banking sector (see table 2), although banks have, generally, undertaken some de-risking programmes.

There are currently 10 operating banks (9 groups), plus one representative office of an overseas bank. The sector directly employs circa 2,000 staff. Further information on the sector size is in table 5 below. Additional information on the cross border nature of IOM banking is shown in tables 6a and 6b.

Table 5: key data banking sector (as at Dec 2018)

	Value £bn
Retail deposits (***note A***)	17.4
Corporate / trust / fiduciary deposits (***note A***)	10.9
Deposits / loans from other banks (including group)	9.2
Other deposits	0.3
Total deposits (note B)	***37.8***
Other liabilities (including capital)	1.0
TOTAL LIABILITIES	**38.8**
Loans due from group banks	26.5
Loans due from other banks and other marketable assets	4.3
Customer loans – mortgages (net of past due) (***note C***)	3.0
Customer loans – retail	0.2
Customer loans – corporate / other	4.4
Other assets	0.4
TOTAL ASSETS	**38.8**

- Note A: IoM resident individuals make up approx. 15% of retail deposits by value (10% of total retail and corporate deposits). Other IoM entities make up 26% of total retail and corporate deposits.
- Note B: Sterling deposits make up circa 51% of total deposits by value (this does fluctuate).
- Note C: Mortgages to IoM residents/IoM property make up circa 46% of total mortgages by value.

IoM banks report two types of information on their cross border activity on a quarterly basis:-

- Asset and liability positions by certain currencies and country of residence of the counterparty (BIS statistics); and
- Payment flows to/from the IoM (in sterling equivalent) by final destination country, including total value and number of transactions. Some gaps in this data remain, particularly around completeness of data for flows between IoM and UK.

Table 6a: cross border nature of IOM banking

a) Cross border assets (claims) and liabilities (based on June 2018 data for BIS)

	All reporting countries value US$bn	**IOM banks value (and % of total global) US$bn**
All countries cross border claims (assets)	29,455.6	45.8 (0.15%) (***note A***)

All countries cross border liabilities	26,797.5	34.5 (0.13%) (***note B***)
Offshore centres cross border claims (assets)	4,712.9	45.8 (0.97%)
Offshore centres cross border liabilities	4,633.1	34.5 (0.74%)

- Note A: 65% of claims are on the UK, 2% are EU/EEA (including Switzerland) and 33% ROW
- Note B: 37% of liabilities are UK, 8% are EU/EEA (including Switzerland) and 55% ROW

Table 6b: cross border nature of IOM banking

b) Payment flows[24] (based on cumulative data to Dec 2018 data, 12 months)

	12mth Inflows Value £bn (%)	**12mth Outflows Value £bn (%)**
TOTAL ALL COUNTRIES	**77.0**	**67.6**
Of which UK	*42.8 (55%)*	*35.5 (53%)*
Of which inter IOM	*2.3 (3%)*	*2.2 (3%)*
Of which Channel Islands	*5.3 (7%)*	*2.9 (4%)*
Of which EU	*10.1 (13%)*	*9.2 (14%)*
Of which other Europe	*2.6 (3%)*	*2.9 (4%)*
Of which Americas	*9.4 (12%)*	*8.5 (12%)*
Of which Africa	*2.1 (3%)*	*2.7 (4%)*
Of which Asia (incl. Middle East)	*2.1 (3%)*	*3.1 (5%)*
Of which Oceania	*0.3 (less than 0.5%)*	*0.6 (1%)*
Highest risk countries (29)	**12mth Inflows**	**12mth Outflows**
Total value £bn	0.25	0.30
As a % of total flow	*0.32%*	*0.44%*

Of the inflows from the 29 higher risk countries, 83% by value and 74% by volume are from 5 countries (4 being African). Of the outflows to the 29 high risk countries, 81% by value and 73% by volume are to the same 5 countries as above.

Data from the FIU shows that banks made 56% of all SARs in 2017/18. Only a very small proportion of SARs were for TF and the largest categorization was related to tax.

[24] Payment Flow data is not fully complete, for example not all banks are reporting sterling flows in faster payments / bacs. Also, data quality more generally is still improving.

Vulnerabilities

The nature of banking products and services, and some customer segments serviced (including high net worth individuals, complex structures and PEPs), result in core inherent vulnerabilities. The importance of strong controls is therefore paramount.

There is a wide customer base and the international reach and low tax environment of the IoM creates a risk of ML, for example being used to evade tax, via the use of complex structures in the corporate market. There can be difficulty in establishing source of funds/source of wealth, where complex structures and/or trusts are involved leading to a risk of funds being the product of various predicate crimes, including corruption. The non-face to face nature of the relationships and the use of introducers/third parties (which can also include PEPs) also increases threat. Sanctions risks arise from the international nature of the sector and from exposure to higher risk countries. The IoM has a highly formalised economy; nevertheless there is a threat resulting from the use/deposit of cash in particular from domestic laundering from drug related crime.

Banks in the IoM may be vulnerable to ML/TF for the following reasons:

- The international nature of business including non-face to face and use of third parties in the process (including group introductions), potentially making it harder to identify illegitimate business / transactions. However AML/CFT requirements in this area are robust;
- The use and acceptance of cash in the system, albeit noting this is more focused on local resident customers or cash generating local businesses;
- The fast transactional nature of services across a range of currencies, including vulnerability to fraud against customers (i.e. money being taken from accounts);
- Potential for funds to be deposited arising from bribery or corruption due to the international focus and, in some case, complex structures (including involving PEPs), or from proceeds of fraud (not reported) which can be difficult to detect;
- Technology: banks may not have sufficiently robust technology to help prevent and detect money laundering (transactions, screening, changes in customer profile and behaviour) and be over reliant on manual intervention. Or they may have good technology but not understand its use properly, or be too reliant on it as a defence. Technological changes may also make the bank more vulnerable to fraud against their customers (for example cheque fraud). This can be a particular challenge when dealing with fast money transfers cross border (including online) and understanding what is normal vs unusual;
- Banks not understanding their own risks and vulnerabilities to ML/TF through weak or unrealistic business risk assessments.
- Pressure of business, which could result from a group's strategy or approach, for example taking commercial decisions ahead of regulatory concerns.

Overall risk

It is considered that the overall risk for Banking is **Medium** taking into account the threats and vulnerabilities, balanced against the controls in place in the sector. The domestic inherent retail risk (including HNWI) is **Medium** but the international retail (including HNWI) and corporate / trust sector risks are inherently **Medium High**. There are limited instances of the IoM banking sector being potentially used for TF, and ML is considered to be the higher risk.

Collective Investment Schemes (Funds), Fund Managers and Administrators

This section covers the following types of financial services activity:

- Fund management/administration; and
- The business of Isle of Man funds (collective investment schemes)

Fund managers and administrators in the IoM provide services to a range of fund vehicles, both IoM funds, and overseas funds. Fund management and administration is a regulated activity and such firms are licensed and supervised by the IOMFSA under the Financial Services Act 2008 (FSA08). Firms in the IoM that provide asset or investment management services to funds are covered in the NRA under asset and investment management.

Fund managers/administrators' clients are the funds themselves. Fund managers / administrators are responsible for assessing the ML and TF risk associated with taking on funds as clients. This includes an understanding of not only the investor base but also what the fund is investing in, the fund structure, and the other functionaries providing services to the fund.

A key difference in this sector is that all funds established in the IoM under the Collective Investment Schemes Act 2008 are also "relevant persons" for the purpose of AML/CFT legislation; this means the AML/CFT Code also applies directly to IoM funds. In practice the governing body of an IoM fund will delegate the majority (if not all) of AML/CFT matters to its functionaries (fund manager/administrator), but the governing body must understand and document what services the functionary is, and more importantly is not, providing in relation to the fund's obligations under the AML/CFT Code. This should be included as part of the functionary agreement between the fund and the Manager or Administrator.

The underlying clients of funds range from retail individuals (predominantly non-resident) to more sophisticated individual investors and also corporate and institutional investors. Investment into funds is often made through intermediaries, financial advisory firms, investment firms/portfolio managers, custodians, and life companies. Many of these intermediaries are regulated firms outside of the IoM. Some investments are made on a pooled basis and the investments are controlled and managed by those intermediaries. Some investors may pose higher risk or be PEPs.

Fund managers/administrators also operate subscription and redemption accounts (client accounts) to manage money flow and may use IoM banks for this service.

As of 2019 there are 15 firms licensed as fund managers/administrators by the IOMFSA, employing circa 150 to 170 staff. Some TCSPs (15) also provide administration or custodial services to exempt funds; these firms report their fund statistics to the IOMFSA and that data is included in the information below.

Non-retail funds are the most significant part of the sector, and services to IoM funds make up only 52% of the sector by value (but 68% by number), excluding services to closed ended investment companies[25]. There has been limited growth in the sector, with a decline in retail fund business. The main growth has been in exempt funds and closed ended investment

[25] Not all closed ended investment companies fall within the Collective Investment Schemes Act 2008; for these companies, risks identified within the sections on TCSPs and Legal Persons and Legal Arrangements should be considered.

companies, which are also serviced by TCSPs, rather than focussed fund managers/administrators. There has also been an increase in providing administration services to non-IoM managers or administrators.

Table 7: Key funds data - 31 December 2018

	Value of funds (NAV)[26] US$m	**Number of funds**
Retail type funds (authorised and regulated funds, legacy retail)	449	8
Qualifying Funds	227	8
Specialist Funds (non-retail)	1,280	15
Legacy EIFs	223	11
Exempt Funds	3,700	109
TOTAL IOM Funds	***5,879***	***151***
Overseas Funds	3,720	45
Services to overseas managers	1,580	25
TOTAL NON IOM FUNDS	***5,300***	***70***
Closed ended investment companies (not schemes)	6,720	70
TOTAL FUND SECTOR	**17,899**	**291**

In 2017/18 fund and investment managers, together provided 1.0% of the total SARs reported to the FIU (data per FIU).

Vulnerabilities

The Fund Management / Administration sector is mature and has been regulated under the current legislative framework since 2008 with previous regulatory frameworks applying for over 25 years. Even though not always set out in functionary agreements, the experienced managers, administrators and fund governing bodies are aware of their responsibilities of compliance with the AML/CFT Code and reporting suspicious transactions. Most have invested in commercial search engines and undertake regular screening of the funds and their underlying investors.

The main vulnerabilities are:-

- Certain fund types (e.g. retail funds) provide good liquidity characteristics which can increase vulnerability, however these funds are the most tightly regulated and are mature. Investors are mainly UK / Europe and levels of investment are generally smaller value.

[26] Net Asset Value

- Some non-retail funds are more complex in structure and characteristics and may service a particular group of investors (quasi in-house funds); they could be used in the layering process, or may be more prone to fraud. They may also have a higher risk appetite when selecting the investment type, and the functionaries they use (e.g. investment managers outside of the IoM).
- There could be gaps in compliance (by the fund) with the AML/CFT Code if the role of the manager/administrator is not fully understood, or documented, by the governing body of the IoM fund, resulting in potential weaknesses in the system. Robust documentation in this respect is important, and the experience of fund directors and the Managers/Administrators.
- Exempt schemes may be more likely than the other IoM fund types to be used to obtain tax benefits for certain asset types, for fraudulent purposes, or to conceal beneficial ownership (as they are currently not subject to the beneficial ownership registration framework even where there are only a small number of investors/controllers). Further, the legislative framework for exempt schemes is such that there can be few links with the IoM[27] other than, in some cases, a registered agent service provided by a TCSP, or a registered office address. It can be unclear who is undertaking the necessary work to make sure such schemes are complying with the AML/CFT Code. There is no obligation to report the existence of an Exempt scheme to the IOMFSA if there is no IoM regulated entity associated with the fund.
- For services provided to overseas funds, if there is an AML/CFT issue with that fund, any sanction against the fund is the responsibility of the overseas regulator. The IOMFSA's powers would address the IoM regulated functionary only, but the issues may not be at the fund provider level. There could be adverse reputational impact for the IoM.
- The non-face-to-face nature of the sector, use of intermediaries (including pooling), exposure to higher risk jurisdictions and the possibility of integrating small amounts can be a feature of parts of the sector which can pose additional risk, however the AML/CFT requirements as to when any concessions can be utilised by firms are robust.

Overall risk

The level of risk for ML and for TF is considered to be **Medium** based on the profile of the sector, its products and services and control environment. There are some risks posed by the investor base and some scheme structures can be more complex. Further, reliance is placed on third parties for aspects of CDD. However, entry controls are strong, and there is a program of supervisory inspections being conducted that includes assessment of AML/CFT, and the role of fund managers/administrators and governance of funds. This latter piece of work will lead to further sector feedback by the IOMFSA, and improvements in the guidance issued to the sector.

In addition to the future feedback and enhancements to sector guidance, the IOMFSA has recognized there is currently some increased risk in the area of exempt schemes (referenced in the vulnerabilities above) which requires additional attention, which could include regulatory change.

[27] For example no requirement for IoM resident directors or an appointed IoM administrator.

Investment Business: Asset and Investment Management

Including stockbroking, asset and investment management to collective investment schemes.

The provision of asset and investment management services (including stockbroking and such services to collective investment schemes) is a regulated activity. Firms are therefore licensed and supervised by the IOMFSA under the FSA08. The business undertaken in this sector includes asset and investment management services for individuals (including HNWIs), corporations, funds and other FIs. These businesses control and manage their clients' funds including on a discretionary basis.

Business is often non-face-to-face, and could be introduced (third parties). It can also involve larger and more complex transactions and HNWIs (including PEPs). Some parts of the sector are also using technology more in the delivery of their services. Generally, the sector is mature with good quality systems in place, and a strong control environment. Funds received and paid out are normally through bank transfers (although cheques may also be used) and many firms use the local banking system (as a gatekeeper) for this.

There are currently 19 firms classified as investment/asset managers (including stockbrokers) by the IOMFSA, employing circa 250 to 300 staff. In addition, a limited number of banks also provide investment management services within their product suites. Assets under management (excluding firms who the IOMFSA report under fund managers/administrators but also hold other assets) are circa £13bn (as at Dec 18). Over 80% of this is non-retail business and nearly 60% is non-IoM.

Table 8: Key investment data - 31 December 2017

	Value	% (where relevant)
Number of customers	12,499	
Of which higher risk	364	2.9%
Of which PEPs	169	1.4%
Of which IOM resident ***(note A)***	5,360	43%
Of which UK resident ***(note A)***	2,287	18%
Of which other residency ***(note A)***	4,852	39%
SARs made to FIU ***(note B)***	9	
Enquiries from law enforcement	2	

Note A: Residency includes corporate residency for this purpose.
Note B: In 2017/18 fund and investment managers, together provided 1.0% of the total SARs reported to the FIU (data per FIU).

Vulnerabilities

The main vulnerabilities are:-

- A firm could be involved in the chain (layering) of proceeds of crime being moved in the financial system, particularly if products permit early encashment/redemption features (liquidity features). Monitoring of such activity is a key control.
- The sector can deal with higher value customers/more complex transactions which can disguise the true origin of the funds and wealth – particular care is needed in this area especially where income incentives for the firm may be higher.
- The use of pooling is a feature of the sector which can pose additional risk; however the AML/CFT requirements are robust in this area as to when any concessions can be utilised by firms.
- Although technology can assist in preventing financial crime, it can also increase vulnerabilities if not managed appropriately or not understood; it can also lead to faster transaction times, which can be attractive to money launderers. Firms need to be aware of this risk.
- The sector could be prone to market manipulation/fraud although there has been little evidence to show this is a problem.

Overall risk

The level of risk for ML and TF is considered to be **Medium** based on the profile of the sector, its products and services and control environment.

Investment Business: Financial Advisory Firms (FAs)

The provision of, advising on, and arranging deals for investments is regulated activity. Financial advisory firms ("FAs") are therefore licensed and supervised by the IOMFSA under the FSA08. Some of these firms are independent financial advisers.

FAs in the IoM generally undertake business on a face-to-face basis, providing advice predominantly to IoM resident clients. They do not hold or manage client money in respect of investment business. Money being settled into an investment product recommended by an FA will pass from one regulated business to another, but not to or from the FA. As part of their responsibilities to provide suitable advice, FAs must fully understand their clients and their needs, and their wealth, and assess the ML/TF risk. There is very limited reliance on third parties for CDD collection, or the use of introducers. Strong entry due diligence controls are in place.

There are currently 15 firms licensed as FAs by the IOMFSA, employing circa 120 staff. In addition, some banks also provide limited financial advisory services to their customers.

Table 9: Key FA data - 31 December 2017

	Value	**% (where relevant)**
Number of customers	25,036[28]	
Of which higher risk	*152*	0.6%
Of which PEPs[29]	*57*	0.2%
Of which IOM resident	*22,691*	91%

[28] Many of these customers will be for business written in previous years, and some customers will appear more than once.
[29] Mostly domestic.

Of which UK resident	*2,062*	8%
Of which other residency	*283*	1%
SARs made to FIU	3	
Enquiries from law enforcement	1	

Vulnerabilities

The main vulnerability is that an FA could be involved in the chain of arranging for proceeds of crime to be moved/settled into a legitimate product. Some small FAs can have difficulty in segregating the compliance and Money Laundering Reporting Officer (MLRO) roles from operational/financial adviser staff. However, this is countered by the generally strong controls in place and the maturity of the sector.

Overall risk

The level of risk for both ML and TF is considered to be **Low** based on the role and nature of FA business, the predominantly local resident client base level of activity, and the requirements in place to understand clients and their financial circumstances.

Insurance Sector – Life and Non-Life

The insurance sector is the largest financial sector in the IoM, contributing 17.6% of national income in 2017/18. It is a well-established and mature industry. At 31 March 2019 there were 13 authorised long term (life) insurers, 104 authorised general (non-life) insurers and 16 permitted insurers[30] with £ 66.2 billion of funds under management in the life sector and £6.3 billion in the non-life sector. Approximately 2,000 people (3.9% of the working population) work in the Insurance sector, 83% of which are in the life sector.

The insurance market in the IoM itself is represented by a number of industry and professional bodies e.g. bodies acting on behalf of long term insurers, captive managers, and insurance brokers.

In 2017/18 the combined insurance sector submitted 9% of ML SARs to the FIU; the joint third largest contributor by sector. In respect of TF SARs, the life sector was the largest contributor with 4 SARs representing 57%.

Life Sector

Life assurance companies in the IoM are, in the main, subsidiaries of large internationally active groups head-quartered in the UK or Europe. The life sector consists of authorised and permitted insurers writing predominately long term unit linked business, where policyholder liabilities are directly linked to the performance of an underlying financial asset. Approximately 99.5% of liabilities within the life assurance sector are unit linked.

IoM life companies are predominantly internationally focused targeting HNWIs and mass affluent customers, including expatriates and non-resident customers. The IoM domestic market is insignificant. Geographically the largest exposure remains to insurance business written into the

[30] Permitted insurers represent branches on the Island of insurers licensed in a jurisdiction other than the Island

UK, although a number of firms continue to distribute products internationally to the Far East, Middle East, Africa and Latin America and as a result the geographical representation of sales is extensive.

Products are sold predominately on a non-face-to-face basis through IFAs. Whilst life companies collect evidence of CDD through IFAs, this service is provided in accordance with terms of business with the insurers being obligated via the AML/CFT Code, to satisfy themselves as to the identity and verification of identity of the customer and beneficial owners.

Insurance companies have a high level of understanding of the inherent risks related to investment products sold on a cross-border, non-face-to-face basis. On the whole, companies understand their obligations and there are well-established and tested measures in place to mitigate risks.

Vulnerabilities

There is a risk that the funds used to purchase life insurance may be the proceeds of crime. There is also a risk, albeit limited, that funds withdrawn from life insurance contracts could be used to fund terrorism. The main vulnerabilities facing the Island's life assurance sector are:

- Whilst many life insurance products are not sufficiently flexible to be the first vehicle of choice for money launderers, a significant proportion of products sold by IoM life insurers are aimed at the high net worth individual and can provide highly personalised features increasing the flexibility and inherent vulnerability of the products sold.
- The highly personalised nature of certain bonds which permit a wide range of asset investments could provide a mechanism which may impact the traceability of ownership. The assets are legally and beneficially owned by the life company who are responsible for UBO due diligence.
- The international nature of the business, including non-face-to-face and use of third parties, potentially making it harder to identify illegitimate business/transactions;
- The use of legal persons and arrangements such as trusts both as asset-holding vehicles and as part of more complex structures to obscure the beneficial owner of the product;
- The prevalence of cross border transactions, including from jurisdictions with weak preventative measures in place reducing the reliability of the evidence provided by IFAs;
- The risk that commission may override focus on preventative measures as applied by the IFAs.

Risk

Whilst FATF[31] note that generally the ML/TF risks associated to the life insurance sector are lower than that associated with other financial products, the indicative inherent risk rating at a product level (see FATF table 9 which includes each product type) is before any other risk factors which may also have a bearing on the inherent risk such as transaction, distribution, geographical or customer risks.

[31] FATF Guidance for a risk-based approach for the life insurance sector – October 2018

Table 10: FATF risk ratings for Life Products

EXAMPLE OF PRODUCT DESCRIPTION	TYPICAL FEATURES	INDICATIVE RISK RATING
Complex products with potential multiple investment accounts; and /or products with returns linked to the performance of an underlying financial asset ***Example of product names*:** Universal Life Variable Universal Life Wrapper Insurance Investment Linked Policies Unit Linked Policies Investment Linked Assurance Schemes	• offers the ability to hold funds and/or assets • may offer the option of asset transfers into the policy • full or partial underlying investments under control of the customer • may have a high upper limit for the amounts of funds held	**Higher risk** compared with other life insurance products
Products designed for High Net Worth (HNW) persons or products for individual generally with guaranteed returns ***Example of product names*:** HNW Individual Life Insurance Traditional Whole Life	• offers the ability to hold funds • only with high limit for funds held • underlying investments managed by the insurer	**Higher/moderately high risk** compared with other life insurance products
Product subscribed by a company to pay a periodic income benefit for the life of employees ***Example of product name:*** Group Annuities	• typically used for retirement savings and pension schemes • generally subscribed by a company in order to provide a future benefit to its employees • underlying investments managed by the insurer	**Lower risk** compared with other life insurance products
Product that pays a lump sum, or a regular pay out (annuity) to the beneficiary, in the event of the death of the insured, in the event of a long-term care or critical illness ***Example of product name:*** Term Life Individual Group Long-term Care Critical Illness	• no ability to hold funds • generally payments only in case of a specific external event	**Lower risk** compared with other life insurance products

The product risks identified by FATF, when considered in the light of the other vulnerability factors present in the Island's life assurance sector, are consistent with the assessed inherent risks for each of the product types. Overall, after applying consideration of the control and other preventative measures in place, together with the product weightings, the life sector is assessed as having a **Medium** level of vulnerability for ML and a **Medium** level of vulnerability for TF.

Non-Life Products

The Non-Life Sector consists mainly of captive (related party) insurers. At 31 March 2019, there were 104 authorised Non-Life insurers of which 75 write purely related company insurance business. The shareholder organisations for this sector are largely national or international listed companies. The sector also includes one third party insurer of general insurance business focussed solely on the domestic market.

Captive insurance contracts mainly provide protection for group owned assets and liabilities with share capital, premium inflows and claim outflows being largely between group companies. The majority of premium outflows are to the reinsurance sector, much of which is placed in the London and Lloyds' insurance markets. Significant claims generally involve the appointment of an independent loss adjuster who will verify the claim and advise on reserves and settlement values. The captive insurance companies are in the main managed by regulated insurance managers who together with the required appointments of independent non-executive directors provide independent oversight and governance arrangements for this sector.

Vulnerabilities

Whilst FATF consider that general insurance and reinsurance are not completely immune from criminal infiltration, there are various instances of crimes which may not be confined to mere instances of fraud, but possess all the measures of ML e.g. a risk of corporate structures (such as insurance or reinsurance companies) being set up in order to channel funds to disguise their original source. International typologies in the non-life sector identify the following vulnerabilities which are relevant:

- General insurance claim fraud involving high value goods purchased with illicit funds;
- The use and acceptance of cash for the payment of premiums, albeit noting this is more focused on local resident customers purchasing statutory general insurance cover;
- Cooling off periods, which allow for refunds of premium with clean money within the contract cancellation period;
- Collusion of customer, intermediary and/or insurance company employees;
- Third Party payments of premium;
- Risks involved in international transactions – both where this is source of business or a destination of policy payouts;
- Fraudulent customers, insurance companies and reinsurance companies.

Risk

The non-life sector which represents 7% of the overall insurance sector is assessed as having a **Medium Low** vulnerability to ML and TF. This reflects the lower risk profile of the products offered by this sector.

Overall Insurance Risk

The composite risk rating of the two sectors mirrors that of the life sector which is **Medium** for ML and also for TF as the life sector dominates the insurance sector both in terms of size of the sector and those products that represent a higher vulnerability.

Pensions

The private pensions sector in the IoM is well established; in order to be authorised by the IOMFSA schemes may only be provided by way of irrevocable trust structures. These schemes are authorised as either Domestic schemes (for those habitually resident in the IoM) or International schemes (for all other non-domiciled persons/entities) and require the appointment of trustees who have demonstrated to the IOMFSA that they are fit and proper in accordance with the IOMFSA's regulatory standards.

The appointment of an Administrator who is responsible for the management of the scheme and who has similarly demonstrated their fit and proper status is also required, and these must be registered with the IOMFSA after having demonstrated that they have sufficient knowledge and experience to manage the scheme. Where scheme Administrators are registered as Professional this recognises that they operate by way of business and generally manage multiple schemes. In-House Administrators are so registered where they act in respect of only one scheme and not by way of business.

At 31 March 2019 there were 48 Administrators registered with the IOMFSA (18 Professional and 30 In-House); currently the AML/CFT legislation applies solely to Professional Administrators, who employ approximately 110 people.

There were 1,134 authorised schemes (986 Domestic and 148 International) with assets in the region of £10 billion. Domestic schemes are predominantly personal and distribution is primarily via direct customer contact or referral by independent financial advisor. International schemes are predominantly occupational and distribution is primarily via intermediary and/or financial advisor.

Table 11: key private pensions data – January 2018

Scheme Type	**"Master Trust"-style**		**Other types of Scheme**		**Total**
Occupational	**Domestic**	**International**	**Domestic**	**International**	
Number of Schemes	4	7	122	109	**242**
Number of Members	57	6,820	8,385	90,240	**105,502**
Number of Participating Employers	9	24	138	177	**348**
Number of customers assessed as higher risk	0	1	0	11	**12**
Number of customers assessed as standard risk	28	20	22	115	**185**
Number of domestic PEPs					**3**
Number of foreign PEPs					**99**
Personal					
Number of Schemes	37	14	708	19	**778**
Number of Members	4277	730	884	19	**5910**
Number of customers assessed as higher risk	19	0	7	1	**27**
Number of customers assessed as standard risk	2858	468	1784	64	**5174**
Number of domestic PEPs					**27**
Number of foreign PEPs					**13**

Vulnerabilities

The main money laundering vulnerabilities of private IoM pension products tend to arise from personal schemes with complex underlying investment structures or taxation arrangements; these may be vulnerable to the disguise of the proceeds of fraud and/or tax evasion. Terrorist financing vulnerabilities tend to originate with large International occupational schemes which see participating employers and employees/members located around the world.

Although there is a high level of awareness of the immediate origin of monies transferred into a pension scheme by the sector, particularly as much of this money will originate from pre-existing pension arrangements, there may be an over-reliance on the previous scheme's legitimacy by Administrators in the due diligence process. Also, whilst there is a high level of awareness of traditional terrorist financing methods, there is an over-reliance by Administrators on the due diligence undertaken on a scheme employer itself as an indicator of the total customer risk ascribed to a scheme.

Overall Risk

The sectoral risk for private pensions in the IoM is **Medium Low** for both ML and TF**.** These are products which tend to see funds inaccessible for longer periods of time and do not generally offer the level of flexibility needed to be attractive for traditional ML purposes, however it is recognised that ML and TF risks remain and that the sector requires special consideration in respect of its exposure to the risks of tax evasion and fraud.

Other Financial Institutions (excluding moneylenders)

This section covers the following types of financial services activities:

- Money transmission services: payment services directly and e-money providers
- Money transmission services: bureau de change, payment services as agent, cheque cashers
- Credit Unions
- Loan / Equity Crowdfunding

Overview

Overall, the Other Financial Institutions (OFI) sector is small compared to other financial sectors such as banking. All OFI sectors are licensed and supervised by the IOMFSA under the FSA08 with the exception of the Isle of Man Post Office, which is exempted from holding a licence, although it is still subject to AML/CFT oversight from the IOMFSA.

Money Transmission Services: Payment Services Directly[32] / E-money

There are only 2 firms licensed by the IOMFSA for payment services directly. There are currently no e-money firms. The IOMFSA is in discussion with potential new market entrants in this sector. The 2 current payment service firms have quite distinct business models from each other. Sectors served include gaming, foreign exchange/trading houses, and some TCSPs (for example as an

[32] Payment Services Directly refers to entities that are licensed for class 8(2)(a) regulated activity as the principal person that holds client funds in segregated payment accounts.

alternative to traditional banking). Some customers are considered higher risk, and there are also some PEP relationships.

Some payment service firms may also attract, or even target, customers who may not be accepted by banks directly. Firms are also often smaller with no large group infrastructure and may be reliant on a small number of clients for income generation.

The money flow from the 2 operators is however quite large in isolation (circa £1.5 billion per annum), although small compared to the banking sector. It is therefore important that these firms have robust monitoring systems in place to help identify risks, akin to those used in banks. They must also hold client funds in segregated payment accounts with banks.

Table 12: Key data OFIs (2 firms combined)

	2018	**2017**
Annual cumulative turnover	£1,570 million	£1,602 million
Payment service users (approx.)	127	126

In 2019 the IOM Post Office also launched a new targeted "cash transmission service". The IOM Post Office is exempt from holding a licence but must comply with the AML/CFT legislation. Additional reporting is to be put in place between the IOM Post Office and the IOMFSA in relation to this new service.

Vulnerabilities

Key vulnerabilities include:-

- One firm is heavily reliant on one client for its business revenues (reliance on a small number of clients for income can be a more general vulnerability);
- Could be used to move funds generated from crime quickly round the financial system, for example through technological solutions (can be attractive to criminals);
- Clients may be higher risk, and cannot get banking direct;
- Clients are often non-face-to-face.

Overall risk

Level of risk for ML and TF is considered to be **Medium** based on the level of activity conducted and the client base, noting the monitoring and screening controls in place. The addition of further providers in this sector may increase the risk profile.

Money Transmission Services: Bureau de Change, Payment Services as Agent, Cheque Cashers

There are 3 providers of bureau de change in the IoM (a further provider surrendered its licence in 2019), including the IOM Post Office. 2 of these firms also operate payment services in an agency capacity, one for Western Union and one for MoneyGram. There are no cheque cashers.

Annual statistical information is obtained from these firms, and the size of the sector is relatively small.

Table 13a: Key data Bureau de change

	2018	**2017**
Volume	36,839	40,568
Value	£11,568,527	£10,814,710
Average transaction	*£314*	*£266*

Table 13b: Key data Agency services

	2018	**2017**
Funds sent volume	5,442	6,247
Funds sent value	£1,315,286	£1,577,734
Average transaction	*£242*	*£252*
Funds received volume	448	400
Funds received value	£154,033	£148,541
Average transaction	*£344*	*£371*

Business is conducted face-to-face and mostly with residents of the Isle of Man. Majority of transactions are of small to average value with controls in place to check and verify higher value transactions. There is evidence of internal disclosures being made in one firm and reporting to the FIU (and enquiries from law enforcement). This is more focused on agency business. There have been no material changes since the 2015 NRA.

Vulnerabilities

The main threat is low level domestic laundering using cash, as many transactions fall under the CDD thresholds to verify the identity of the customer (an exempted occasional transaction). Further, agency business provides a route to move cash to/from other jurisdictions, including the UK (e.g. low level drug trade) and therefore results in a wide geographical reach.

There is also the potential threat of money being sent to higher risk jurisdictions through agency business that could relate to TF. To combat this, firms need a good understanding of ML/TF relevant to bureau de change and agency operations. There is a risk that staff training and knowledge in this sector is not robust enough. However, the majority of countries to which money is sent from the IoM are consistent with the domestic population having familial links to those countries. Based on data received from providers, the IOMFSA may raise queries/request evidence in the event money is reported as being sent to a jurisdiction that may pose a higher risk of ML/TF.

Overall risk

The level of risk for both ML and TF is considered to be **Medium Low** based on the low value and transactional activity conducted, the predominant nature of the customer base (local residents) and the level of controls and oversight arrangements in place for a sector of this small size. It is recognized that agency business poses some additional risk for both low level ML and potentially TF.

Credit Unions

The operation of a credit union became a regulated activity under the FSA08 with effect from 1 April 2019. Credit Unions were already subject to the AML/CFT Code before this date, and are also subject to the provisions contained in the Credit Unions Act 1993, as amended ("CUA"). There is currently one credit union in the IoM, with total member funds of circa £500k.

The CUA restricts the level of business. Firstly, members must have a common bond and be resident in the IoM. Secondly, members can only hold ordinary shares of up to £5,000 value and borrow up to £5,000 more than they hold in shares. Business is mainly conducted on a face-to-face basis.

Vulnerabilities

Cash can be accepted which is a potential vulnerability especially if a prepaid card facility is added to enable added functionality. However, there are limits on value in law and limits a credit union will place on cash activity. A credit unions' target market will include persons who may have difficulty accessing banking services.

Credit unions are volunteer run organisations and may therefore lack the level of discipline or the training available to professional firms; they are also reliant on others to support them, for example other banks, and has limited resources.

In terms of controls, procedures are in place to combat money laundering, and the credit union also has access to resources of the UK trade body of which it is a member. Credit unions must also have an internal audit type function to help oversee compliance.

Overall risk

The voluntary nature of the sector and the make-up of the client base slightly raise the risk although there is a borrowing limit of £10,000. The overall ML and TF risk is considered to be **Medium Low**, based on the low value and limited transactional activity conducted, the size of the sector, and the nature of the customer base (local residents).

LOAN / EQUITY CROWDFUNDING

Currently there are no firms licensed in this sector.

7. Designated Non-Financial Businesses and Professions

- Accountancy Services - Accountants and Payroll Agents
- Legal Services – Advocates and Registered Legal Practitioners
- Gambling – Online and Terrestrial
- Trust and Corporate Service Providers
- Convertible Virtual Currencies
- Estate Agents

- Non Profit Organisations
- Moneylenders
- High Value Goods Dealers

Summary

Non-financial services have seen significant growth in recent years; online gambling now forms the largest contributor to National Income in the IoM at 21.1%. Gambling (online and terrestrial) has its own regulator in the IoM, the GSC. Other significant non-financial services sectors include trust and corporate services providers (TCSPs) and legal and accountancy services. External accountants make up the largest number of individual registrations at around 48% of the total (excluding TCSPs and Gambling).

The provision of Trust and Corporate Service Provider services is a regulated activity and as such firms are licensed and supervised by the IOMFSA under the FSA Act 2008. CSPs have been regulated since 2000 and trusts since 2005.

Other sectors which are considered in this report are real estate services, high value goods dealers (HVGDs), payroll, convertible virtual currency, moneylending and NPOs. HVGDs, NPOs and moneylending in the IoM are considered low risk in respect of ML. NPOs are internationally recognised as being at risk of abuse for TF however there has to date been no evidence of this in relation to IoM NPOs and registered charities.

There has been growth in crypto-currency and there are now 30 registered crypto businesses operating in the IoM.

The AML/CFT legal framework for all businesses in the regulated sector is robust and has recently been expanded with the introduction of a civil penalty regime for Code contravention which applies to all businesses in the regulated sector[33].

Guidance (including sector guidance) is currently being updated for all financial and non-financial sectors, in consultation with all relevant stakeholders following the adoption of a new AML/CFT Code in 2019[34].

Accountancy Services – Accountants and Payroll Agents

Accountants

The accountancy sector in the IoM ranges in size from sole practitioners to the offices of large international practices and provides bookkeeping, audit, tax and advisory services but is not generally involved in property transactions. Tax services, including advice on structures and the mitigation of tax liabilities can be provided by accountants but also by legal professionals and in-house experts in TCSPs.

The accountancy sector in the IoM is large; in May 2019 162 businesses who undertake accountancy work were registered as designated businesses, making up 48.4% of businesses registered under the Designated Businesses (Registration and Oversight) Act 2015.

[33] As included in Schedule 4 to POCA 2008

[34] Including the introduction of the Gambling AML/CFT Code which covers terrestrial as well as online gambling.

The activities of external accountants, audit services and tax advisers are designated under Schedule 4 to POCA 2008 as undertaking business in the regulated sector. As such they are required to comply with the requirements of the AML/CFT Code. The activities of this sector are also included in the Designated Businesses (Registration and Oversight) Act 2015 (DBRO Act), giving the IOMFSA the power to oversee the sector in relation to AML/CFT compliance.

The accountancy sector is covered by a large and diverse number of professional bodies. The IOMFSA has delegated oversight agreements in place with a number of professional bodies; members of these bodies can elect to have the oversight of their AML/CFT compliance undertaken by these bodies. Where professionals choose not to elect to have oversight conducted by such a body, the IOMFSA remains responsible. Inspections undertaken by professional bodies are conducted in accordance with IOMFSA guidance, findings are reported to the IOMFSA, joint inspections are conducted and working papers made available to the IOMFSA on request. Only the IOMFSA has the power to take enforcement action. The IOMFSA has delegated oversight agreements in place with the following professional accountancy bodies;

- The Institute of Chartered Accountants of England and Wales
- The Association of Chartered Certified Accountants
- The Institute of Certified Bookkeepers
- The Institute of Financial Accountants
- The International Association of Bookkeepers

Of the 162 accountants registered as designated businesses, 65 (40.1%) have elected to be overseen directly by a professional body.

Oversight inspections have shown that the larger firms within the sector are more likely to have a detailed knowledge of the AML/CFT legislation, and to have access to group wide compliance and internal audit systems. Whilst smaller firms may not have this level of technical AML/CFT knowledge, the majority of their business is conducted face-to-face and there is a detailed knowledge of the customer.

Many businesses in the accountancy sector in the IoM do not hold client monies or become involved in client transactions; for example they provide bookkeeping or audit services only. These companies have a lower risk of being actively involved in ML/TF, and are well placed to identify and report issues. It is a perceived view that because accountants do not generally handle client funds, the ML risk is not significant; however there are other risks attendant upon the sector which do not relate to handling monies.

During the period 1 April 2018 -31 March 2019 the FIU saw an increase in the number of SARS submitted from the accountancy sector to 24, this equates to 1.3% of all the SARS submitted[35]. It is possible that some SARs from the sector may appear to be submitted via TCSPs and this is something that the FIU will be looking into. The number of businesses in the accountancy sector registered on the FIU on-line reporting system also increased during the period and 94% of businesses are now registered.

There have been no instances to date of an accountant in the IoM being prosecuted specifically for ML; there have been a number of cases of accountants being successfully prosecuted in recent years for other financial crimes, for example fraud and theft of client monies. In such cases the IOMFSA considers and takes the most appropriate action against the business and/or the

[35] In 2017/18 Accountants submitted 1.0% of all SARs.

individual. The role of accountants as professional facilitators should be given appropriate consideration in line with the experience of other jurisdictions.

Given the number of sole practitioners, it is possible that there are accountants who have not registered as Designated Businesses. Undertaking designated business without being registered is an offence, and during the year 2018-2019 the IOMFSA issued two civil penalties of £5,000 to businesses who had carried on accountancy work without being registered. It has also been identified that there may be a number of accountants undertaking unregulated TCSP activity, in these cases the IOMFSA is investigating and regularising the positions.

Vulnerability

The accounting sector may be used by money launderers to provide additional layers of legitimacy to criminal financial arrangements, especially where large sums may be involved. Whilst accountants and tax advisors do not ordinarily handle funds, they will often see more of a customer's overall affairs than any other single financial institution or DNFBP. Accountants have knowledge and specific technical abilities which can make them attractive to professional money launderers.

Due to the work they undertake, accountants and tax advisors are more likely to have contact with clients who are HNWI, PEPs or where there are other identified factors known to present ML risks e.g. carrying out certain transactions on behalf of customers and/or providing introductions to FIs. No specific TF vulnerabilities have been identified within the sector.

Certain other activities performed by accountants are more susceptible to ML/TF including;

- Providing tax or other financial advice
- Handling client assets
- Formation of companies and trusts
- Company secretarial services

Overall Risk

The level of risk for ML is assessed as **Medium** because of the factors identified above including the comparative size of the accountancy sector in the IoM, the wide breadth of activities, the range of businesses from sole practitioners up to large international firms and the attractiveness of the sector to criminals. The risk of TF is assessed as **Medium Low.**

Payroll Agents

Payroll agents provide services for businesses including processing payroll calculations, collecting funds from an employer/business, paying the net proceeds to the employee/contractor, ensuring accurate payroll tax and deductions, generating and distributing electronic payroll records and handling payroll compliance matters. There are no specific professional or technical qualifications required to work in the sector and no specific overall professional/industry body in the IoM.

The business of a payroll agent is included in Schedule 4 to POCA and therefore payroll businesses must comply with the AML/CFT Code. Payroll activities are also registrable under the DBRO Act 2015. The IOMFSA therefore has the power to oversee the sector in relation to AML/CFT compliance.

Whilst a comprehensive AML/CFT regime was in place for payroll businesses for some time, it did not cover situations where a contractor was employed by the payroll company, which was a large proportion of the sector. This was rectified by an amendment to the definition of "payroll agent" which was made in to Schedule 4 of POCA and Schedule 1 of the DBRO Act 2015 and which came into force on 1 June 2019. The amended definition now covers the situations where:

- The payroll agent is not the individual's employer;
- The payroll agent is the individual's employer but the place of work of the individual is outside the Isle of Man;
- The work being carried out by the individual is not being carried out directly for the payroll agent or any company within a group to which the payroll agent belongs and;
- The work being carried out by the individual is not the principal trade or business of the payroll agent.

In September 2019 there were 12 standalone payroll agents registered with the IOMFSA. An additional 6 standalone payroll agents were registered but have since de-registered. There have been no additional registrations since the amended definition of 'payroll agent' came into effect. DNFBPs can register as more than one type of designated business; the number of businesses who have registrations which include the activity of 'payroll agent' is 60.

The same civil and criminal sanctions apply to payroll agents as to the rest of the DNFBP sector. The IOMFSA undertakes the oversight inspections of DNFBPs on a risk based approach. In 2018 the IOMFSA focussed their inspections on sectors perceived to be of higher risk, including the payroll sector. The IOMFSA have undertaken inspections to 6 registered payroll agents; these inspections have shown that the AML/CFT knowledge of staff is generally good and no significant issues have been identified regarding the effectiveness of compliance systems. There is however a tendency to discount the risks inherent to the sector.

As of September 2019, of the 12 stand-alone payroll agents and the 60 organisations which have included 'payroll agent' in their DNFBP registration 53 were registered with the on-line SAR reporting system. Between January 2016 and April 2018 the companies who were registered made 18 disclosures the majority of which variously concerned fiscal matters, fraud/false accounting/forgery and CDD issues.

Vulnerability

Payroll agents can be vulnerable to ML in a number of ways, for example;

- Proceeds of crime paid to an employee or contractor by an employer, when the criminals are in fact both parties. Undertaking CDD on both parties and establishing the source of funds and where applicable, the SOW, will help to address this risk.
- The creation of 'ghost' employees by fraudsters using either real or fabricated personal details. Careful auditing of the amounts of the payroll, number of employees etc. is therefore required.
- Receipt of proceeds of crime, bribery or corruption.
- Abuse for tax offences.

Payroll agents should take particular care where customers conduct non face-to-face business or use intermediaries without good reason, or where there appears to be an attempt to disguise the

real owner or related parties. Also where the customer has a record for, or is known to be investigated in respect of, acquisitive crime. Other risk indicators include;

- Significant cash contributions.
- Unusual source of funds, with no reasonable explanation.
- Multiple bank accounts or foreign accounts.
- Finance provided by a lender with no reasonable explanation.
- Large increases in payments with no reasonable explanation.
- Large financial transactions which do not appear to have a justified reason.
- Customer requests complex arrangements to be put in place without a rationale.
- The required service was refused by another service provider or the relationship terminated.
- Duplicate names, addresses and NI numbers on the payroll.
- Fluctuations in the amount of payroll expense for customers, which could indicate ghost employees.

Overall Risk

The level of risk for ML is assessed as **Medium** for Payroll services because of the factors identified above including the comparative size of the sector in the IoM and existing typologies. There are currently no typologies in respect of the use of payroll agents for TF; payroll does not appear to be a preferred route for TF and therefore the risk of TF is assessed as **Medium Low.**

Legal Services – Advocates and Registered Legal Practitioners

Overview

The legal profession in the IoM is made up of Advocates and Registered Legal Practitioners (RLPs).

The Manx Bar is a fused profession of solicitors and barristers, referred to as Advocates. In March 2018 there were a total of 239 practicing Advocates employed across 39 practices. The range of services provided by Advocates include wills and probate work; litigation; family law; corporate and commercial work and conveyancing.

There are 6 RLP firms in the IoM registered under the DBRO Act 2015. RLPs provide broadly similar services as Advocates, but cannot undertake conveyancing or appear in court.

Advocates and RLPs are bound by the AML/CFT legal framework when undertaking specific activities which are defined within Schedule 4 of POCA 2008.

Legal professional privilege does not negate the obligations placed on Advocates and RLPs to comply with the AML/CFT legal framework and submit suspicious activity reports (SARs).

30 Advocates practices and 6 RLPs are currently registered under the DBRO Act 2015. The Isle of Man Law Society is the delegated oversight body for 30 registered businesses and the IOMFSA oversees the 6 designated businesses in this sector. Table 14 below provides a breakdown of the % of legal sector business relevant to AML/CFT; the data cannot currently be separated into Advocates and RLPs.

Table 14: Approximate breakdown of designated business activities carried out by Advocates and RLPs[36]

	Approx. breakdown of designated business activities carried out by Advocates and RLPs					
	Managing clients assets	**Sale or purchase of land**	**Managing bank accounts**	**Promotion formation of structures**	**Sale or purchase of a business**	**Management of a legal arrangement**
Approx. number of open matters 2018	128	5117	29	150	158	421
% of sector business	2.13	85.24	0.48	2.49	2.63	7.01

Advocates

The IOMFSA has delegated oversight of AML/CFT compliance of Advocates to the Isle of Man Law Society under the DBRO Act.[37]. The Law Society has a compliance team which undertakes support and advice, oversight inspections and testing; copies of all inspection reports are provided to the IOMFSA. On occasion the IOMFSA accompany the Isle of Man Law Society on inspections for quality control purposes. In addition, the IOMFSA holds regular meetings with the Law Society to discuss inspection findings and trends within the sector The IOMFSA retains its power to inspect those businesses overseen by the Isle of Man Law Society. Where during the course of an inspection carried out by the Isle of Man Law Society contraventions of the relevant AML legislation are found, these are referred to the IOMFSA for action.

Advocates in the IoM provide the following activities which constitute designated business: managing assets belonging to a client; conveyancing; managing bank, savings or securities accounts; organizing contributions for the promotion, formation, operation or management of bodies corporate; sale or purchase of a business; or the creation, operation or management of a legal person or legal arrangement. Around 12% of the work undertaken is via non-face-to-face instruction; this is largely from law firms in England. Advocates in the IoM are not heavily involved in the formation, registration or administration of legal entities or legal arrangements. Some have separated out TCSP entities from the legal practice into TCSP companies. Advocates accept very limited cash into their practices. Transaction records are easy to monitor and traceable.

Data collected by the IOMFSA confirms that much of the work undertaken by Advocates is from domestic, UK and EU sources. Other work largely arises from FATF equivalent jurisdictions or developed economies. Approximately 80% of designated business activity undertaken by Advocates is domestic conveyancing.

The level of knowledge and awareness of money laundering risk is generally high amongst Advocates. The IOM Law Society and the IOMFSA have a close working relationship and there is an active oversight programme. Thus far the Isle of Man Law Society has conducted inspections on all of the Advocates practices undertaking designated businesses which are under their

[36] Data taken from the IOMFSA statistical return 2018

[37] Advocates were able to elect whether to be overseen by the IOMFSA or the Law Society. All Advocates have elected to be overseen by the Law Society.

oversight; compliance levels are found to be generally strong. The inspection programme looks to carry out inspection on all such practices on a three yearly cycle. The 2016 Mutual Evaluation Report noted that the Law Society uses a risk-based approach to supervising Advocates; the evaluators considered that the Law Society understood the inherent risks within the sector.

In 2017 data collected by the IOMFSA showed that 11% of legal practices were outsourcing their compliance function to non-employees. In respect of reporting suspicions, in 2017/18 Advocates submitted 2.0% of all SARs. This is potentially a little lower than might be expected given the international exposure of parts of the sector. Most SARs submitted were of a good quality, clear and detailed with matters reported promptly.

Vulnerabilities

Criminals, especially criminals involved in high end money laundering, seek to use legal professionals in a number of ways, including;

- Adding respectability to their enterprise, thereby gaining easier access into other parts of the financial framework;
- Using the client accounts of legal professionals to "park" money away from scrutiny;
- Using lawyers to establish legal vehicles (trusts and companies etc. which can then be misused;
- Purchasing of assets, including property, using or disguising the proceeds of crime;
- Using a range of lawyers/legal services to add complexity to transactions and make their origins harder to trace;
- Seeking advice to help facilitate illegal activities e.g. evading tax.

Clients may also use lawyers in order to hide behind legal privilege in an attempt to frustrate the tracing of assets. Because lawyers have specialist skills, knowledge and contacts this can make them targets for such criminality; there are also examples of lawyers being found to be complicit in such cases.

One significant international money laundering typology identified in respect of lawyers – trust and company formation – is not considered to represent a significant risk for Advocates in the IoM. As noted above, the majority of trust and company work is undertaken by separate TCSPs which are regulated and supervised for that purpose. Where Advocates are involved in setting up a trust or acting as a trustee it is essential that the nature and purpose of the trust is known. Further information on these activities can be found under the section on TCSPs.

Purchase of real estate and conveyancing are other areas identified as significant typologies internationally. Conveyancing is a comparatively easy and efficient means to launder relatively large amounts of money. It thereafter provides a legitimate income stream which can be further legitimised by e.g. the payment of local taxes. The 2016 MONEYVAL MER recommended that the IoM conduct a reassessment of risk in respect of real estate and lawyers, which has been undertaken.

Data from the IOMFSA in 2017 showed that 85.2% of the designated business undertaken by Advocate firms involved the sale or purchase of land[38]. In the majority of cases this work is undertaken by officers within Advocate firms who specialise in conveyancing under the supervision of an Advocate.

[38] Where trusts and companies are used to acquire property this is dealt with under the section dealing with TCSPs.

Most conveyancing in the IoM is undertaken on a face-to-face basis and, when an Advocate has a corporate client for conveyancing, additional checks need to be undertaken. Frequent buying and selling by a client or undervaluation of property should act as a red flag and prompt further questions. The Law Society is introducing specific training which will cover all areas of conveyancing work. AML is already covered in AML online training and additional presentations for members and firms.

Other Identified vulnerabilities for Advocates include;

- Client accounts, for example where requirements for transactions are withdrawn by the client, the source of funds changes with little notice, or firms are requested to return funds to the client or a third party.
- Administration of estates where assets have been earned in a foreign jurisdiction or are located in a higher risk territory or there is a suspicion that assets may include criminal property.
- Arranging or advising upon complex cross-border transactions.
- Undertaking company and commercial work.
- Establishment of charities and other NPOs; arranging or advising upon company structures for foreign NPOs.

The UK is the nearest comparable sectoral jurisdiction to the IoM and London firms in particular provide a significant source of work for Manx Advocates. The threats and vulnerabilities faced by UK lawyers and solicitors are therefore considered to be relevant to the IoM assessment with the highest inherent vulnerability being the extent and value of the work provided to high net worth clients, some of whom may also be PEPs. The statistics provided by the IOMFSA shows that Advocates have a high number of clients who are PEPs in the designated business sector in the IoM.

Overall Risk

The exposure to Advocates of being at risk of TF is **Low** for both domestic and international services; neither lend themselves particularly effectively to the facilitation of terrorist financing.

A significant proportion of Advocate work is face-to-face with domestic clients e.g. for conveyancing or family matters. A number of Advocates are involved in international work where there are high net worth clients, a comparatively high number of PEPs and the opportunity for complex business arrangements. There are known typologies internationally. These risks are mitigated by a high level of awareness of money laundering risks within the sector, strong internal compliance controls and an active programme of AML supervisory inspection from the Law Society, overseen by the IOMFSA. The ML risk to Advocates is assessed as **Medium**.

Registered Legal Practitioners

Legal practitioners who are qualified in another jurisdiction (usually the UK), can practice law in the IoM as long as they register under the Legal Practitioners Registration Act 1986. There are prescribed entry controls, which must be met in order to be registered; these include a requirement to hold a prescribed legal qualification which would enable them to practice law in the country in which they are qualified and that they, or a firm of which they are a member or employee, have a permanent establishment in the IoM.

RLPs undertake a range of legal services; they cannot however undertake conveyancing, which work comprises over 85% of Advocate work, nor can they appear in court. Although they are

smaller in number, RLP work involves a higher proportion of designated business and international clients than that of Advocates and includes tax structuring, corporate and commercial law and estate administration. Some RLPs act as 'in-house' lawyers for TCSP clients.

The IOMFSA oversees compliance by RLPs; the IOMFSA has to date carried out 3 inspections

Vulnerabilities

Vulnerabilities for RLPs are the same as those identified for Advocates, except that RLPs do not undertake conveyancing work. International work presents a higher level of risk than work undertaken for domestic clients although this can be mitigated by effective application of CDD requirements.

RLPs should also pay particular attention when undertaking any work involving an international client base where this would fall into the regulated sector as defined by legislation.

Overall Risk

There is less of a comprehensive view of the RLP sector in the IoM than is the case for Advocates who are regulated by the IOM Law Society. RLPs are not regulated by a professional body in the IoM and although the IOMFSA actively engages with those registered there is a risk that some RLPs may not be fully aware of their requirements to register for certain designated activities. There is an action therefore to look at further structured outreach to RLPs by the IOMFSA and FIU. There are smaller numbers of RLPs however they deal with a proportionally higher number of international HNWI. RLPs are assessed as being at **Low** risk for TF and **Medium** risk for ML.

Gambling – Online and Terrestrial

The regulatory authority for gambling activities is the Gambling Supervision Commission (GSC). All gambling, apart from certain limited exceptions is unlawful in the IoM unless licensed by the GSC. The assessment considers online gambling, which is a major sector in the Isle of Man, and terrestrial gambling which is much smaller. The risks for each sector are substantially different.

Online Gambling

Online gambling has been regulated since 2001; the relevant statute governing online gambling is the Online Gambling Regulation Act 2001.

The GSC licences around 45 online operators which offer online gambling to a worldwide player base. As of the end of 2018, the player base is made up of over 4.3 million active players and approximately £1.2bn of players' money was deposited within the final quarter of 2018. The majority of operators are privately owned companies and some of the ownership structures are complex. In 2017/18 e-Gaming accounted for 21.1% of national income. The overwhelming majority of online customers are recreational and deposit small sums in response to promotions and offers of bonuses, although there are also some very significant players where betting and gaming are the basis of livelihoods.

The GSC has legislative powers to determine beneficial ownership and requires all owners to be identified and approved before assuming control or ownership. Inherent risks arise because the industry is by nature non-face-to-face, intrinsically cross-border, operates in a wide variety of

jurisdictions, innovates rapidly and has been an early adopter of convertible virtual currencies. Despite these factors, IoM typology reports for online gambling are relatively rare.

AML/CFT inspections of the online gambling sector have been conducted using risk-based methodologies since Q1 2016 (having previously been conducted without a risk-based methodology). In 2017-18 the e-gaming sector made 18.0% of all SARs to the FIU; this is the second highest reporting sector after banks.

The threat that would be posed by criminal ownership of a licence is significant. The GSC therefore requires beneficial ownership to be disclosed and tests the credibility of ownership during a formal face-to-face hearing where the licence is considered. In addition to its own checks the GSC routinely requests checks by other competent authorities as part of the approvals process. The GSC requires that when ownership changes, new beneficial owners must be approved prior to appointment.

The Gambling (Anti-Money Laundering and Countering the Financing of Terrorism) Act 2018 introduced a broad suite of non-criminal sanctioning powers to the GSC. The Act allows the GSC to add or amend an operator's licence conditions for AML/CFT reasons in order to restrict their activities until satisfied that controls are in place or recommendations or guidance are being complied with. The GSC may also undertake a range of actions to identify failings and issue directions to operators to require them to undertake a specified action, to impose requirements or to require an operator to provide a report to the Commission. Failure to comply with a direction is a criminal offence.

Vulnerabilities

Online gambling is international and non-face to face; the risk factors are countered by a number of factors not least the regulatory framework and supervisory process which are set out above.

There are limited typologies for the online gambling sector relating to large scale or highly organised laundering;

In January 2018 the IOM FIU produced a typology report that included the practice of chip-dumping and another in February 2018 about the use of multiple cards. The GSC conducted a thematic review of multiple card usage which found that this is not a significant issue for the IoM. Most operators have no reported cases of multiple card usage, and of those which have, only a small number are considered suspicious. Another type of fraud occurs when a player loses money using a credit card and then requests a charge-back from the credit card company to effectively refund their losses.

One typology concerns credit card fraud and related identity theft where a fraudster uses stolen credit card details to gamble without risk and then seeks to remove the funds before the fraud is detected. This abuse is largely prevented in the IoM as operators are required to ensure that monies are returned to the same mechanism or a mechanism that the operator is satisfied will result in the customer exclusively receiving the withdrawal.

Auxiliary typologies that have been noted in the public domain include:

- Criminals using online gambling as a leisure activity using the proceeds of crime;
- Match fixers using sites to place legitimate bets on rigged events;

- A thief and/or gambling addict embezzling their company and gambling the money online;
- Criminals offering to purchase VIP accounts that have already been through enhanced due diligence processes, and using these accounts to launder proceeds of crime.

SARs are reported to the FIU in respect of deposits made by players who subsequently do not use them substantially before seeking to withdraw them. This accounts for just under a quarter of all SARs made.

Factors which mitigate the risk of players laundering money through the sector include the fact that the industry is almost exclusively IT based; detailed transaction records are kept and, in most cases, sophisticated perpetual transaction monitoring systems are in place. There are low thresholds over which identity verification is required. This now applies to money deposited as well as withdrawals. A failure to supply credentials typically results in the account being suspended and a Suspicious Activity Report (SAR) being considered.

Overall Risk

There are few domestic typologies available; the online sector is significant, which is taken into account, as have the large number of low risk players and the small proportion of high risk players. The ML risk for online gambling in this assessment remains **Medium** and for TF **Low**.

Terrestrial Gambling

This assessment covers the betting offices operated by bookmakers and the single licensed casino in the IoM. Currently there are 9 betting offices for 3 bookmakers. The number of customers in the sector is comparatively low and the transaction sizes generally small.

The introduction of the Gambling (Anti-Money Laundering and Countering the Financing of Terrorism) Act 2018 updated the legislation concerning terrestrial gambling activities and created consistency across the gambling sector. The 2019 Code requires all terrestrial gambling operators to identify the customer and the source of funds. A €3,000 threshold (stakes and winnings) applies; the operator must verify a customer's identity using reliable, independent source documents, data or information.

The terrestrial gambling sector is highly domestic in nature with most customers well-known to operators. The small size of the IoM means that staff members often know their customers directly or via networks. For certain activities where the casino is licensed to operate activities for business ventures e.g. poker tournaments, there is a requirement to know with whom the business is being conducted.

The customer base of the casino is predominantly domestic although it experiences a modest uplift from the visitor economy. The number of gaming machines and tables for card and dice games is small and occasional, large wins are notable if they exceed £5000. This combined with the small, regular clientele make the casino an unlikely venue for sustained and high-value laundering activity. Quarterly supervisory inspections take place to ensure that the casino meets statutory requirements. There are controls on withdrawals from casino cash desks and player activity on the majority of slot machines and on the tables is monitored and recorded.

Each betting office is subject to an annual on-site check from the GSC which includes reviews of AML/CFT policies and procedures.

There is a vetting process for licence holders, owners and controllers. Fitness and propriety checks are undertaken in line with those for online gambling AML/CFT breaches may be prosecuted under POCA 2008 or under the Gambling (Anti-Money Laundering and Countering the Financing of Terrorism) Act 2018; this Act has introduced a full suite of non-criminal sanctioning powers which extend to terrestrial operators.

The very small size of the sector, low transaction amounts, low domestic crime rates and predominantly local repeat customers act as controls in respect of the known vulnerabilities for the sector. The local Manx currency cannot be spent in the UK and large sums of English, Scottish or Northern Irish notes would stand out as unusual. However it is possible that operators could be misused by requesting winnings or encashment of casino chips in UK rather than Manx currency so that it could be removed from the IoM.

Terrestrial SAR reporting in 2017/18 made up 0.2% of all reports made, suggesting a need to continue to raise awareness.

Vulnerabilities

Known typologies for land based casino betting include:

- Criminal lifestyle spending.
- Collusion, chip dumping, etc. to move funds from one party to another.
- Machines used to launder dye-stained notes[39].

Known typologies for bookmakers include;

- Winning slips used as informal payment mechanism.
- Structuring of bets under threshold amounts at various sites.
- Licenced betting office used to pay in cash which is then transferred to an online account to be withdrawn to a bank, card or payment service provider.

Overall Risk

In 2015 the ML risk for terrestrial gambling was not modelled; this has been addressed for 2019 using the World Bank model, which has resulted in a risk rating of **Medium Low** for terrestrial gambling for ML and **Low** for TF.

Trust & Corporate Service Providers

TCSPs in the IoM are regulated and overseen as FIs with supervision oversight extending to prudential, conduct and governance as well as AML/CFT. Corporate Service Providers have been regulated since 2000. Licensing was extended to include the regulation of Trust Service Providers in 2005. The IOMFSA only licenses TCSPs which offer a full range of regulated activities with TCSP staff being directors or trustees (as opposed to “company formation agents”). Licensing is subject

[39] Where notes exposed to dye e.g. during a robbery, can still be used in a gambling machine.

to an initial and ongoing fitness and propriety test equivalent to that which applies to other regulated sectors. TCSPs have been subject to a risk-based approach to AML/CFT since 2008.

There has been a pattern of consolidation within the industry over the past few years with fewer licence permissions now in force. There are currently 135 licenceholders.

TCSPs on the Island provide a range of services to companies or trusts including aiding company formation and operation. Firms range in size from international businesses with in excess of 100 employees, to small businesses which are in common ownership with the practices of accountants or Advocates and often service a similar underlying client base. Services are provided to just over 30,000 client companies, of which approximately 60% are incorporated in the IoM and 40% elsewhere. In addition, services are provided to over 16,750 trusts. TCSPs in the IoM have the largest amount of gross assets under management of any sector.

The trustees and directors of the entities to which the TCSP provides services have control of assets, investments and bank accounts, and as such TCSPs are important as gatekeepers to the financial system. In common with other FI sectors the business is international in nature with approximately 75% of business originating from the British Isles and EU as detailed in Table 14 below[40]. Shipping, aircraft and property together with ancillary services to online gambling companies feature in many TCSP customer profiles.

Given their wide international reach, TCSPs will have customers from higher risk jurisdictions and beneficial owners with a higher risk profile. The jurisdictional risk profile of customers of TCSPs is similar to the financial services industry as a whole; however, some 5.5% of client companies or trusts are involved with PEPs, compared with an average of 2% across the whole industry.

Table 15: Source of TCSP business

Continental region	Jurisdiction of Beneficial owner	Of which: Higher risk countries (29)
United Kingdom	54.7%	
Isle of Man	9.8%	
Channel Islands	1.1%	
European Union	9,5%	
Other European	4.0%	
Americas	5.3%	0.4%
Africa	6.9%	2.6%
Asia (including Middle East)	7.6%	0.8%
Oceania	1.1%	
	100.0%	3.8%

Consistent with this profile, data collected by the IOMFSA shows that TCSPs have 20% of clients rated by the firm as being of higher risk. This percentage is amongst the highest in the financial services sector.

Annual collection by the IOMFSA of AML/CFT statistical information from all regulated entities has increased knowledge of the profile of AML/CFT risks across TCSPs as a whole, and enabled comparison of a TCSP against its peer group. Other relevant developments include;

[40] Source: 2018 AML/CFT statistical returns: reflects reported place of residence of the beneficial owner

- Establishment of a register of beneficial ownership of all IoM companies under the Beneficial Ownership Act 2017; information from the register is available directly to domestic law enforcement and regulators and to UK law enforcement on request under an arrangement known as the 'Exchange of Notes';
- NPOs sending funds to higher risk jurisdictions ("Specified NPOs") being subject to AML/CFT obligations and required to register under the DBRO Act 2015;
- Monitoring of client money being enhanced through the introduction of a Clients Assets Report.

For further information on types of legal entities and arrangements see Chapter 9.

In 2017/18 TCSPs submitted 9% of all SARs, the joint third highest submissions by sector.

Vulnerabilities

Due to the international nature of the sector, business relationships may not be face-to-face and there may be reliance on third parties; AML/CFT provisions in respect of introduced business have been subject to revision and were further strengthened in 2019 to mitigate this risk.

TCSPs establish and provide corporate and trust structures which can be complex in nature; this is a legitimate activity but complexity provides the opportunity to disguise beneficial ownership, the source of funds and the activities of the entities concerned. The use of TCSPs to provide nominee shareholder activities within complex corporate structures can obscure identification of the true beneficial owner; however this risk is mitigated as the TCSP must know and keep details of ultimate beneficial owners and make these available to competent authorities upon request.

Where TCSPs supply services, including corporate vehicles, for use in international trade there is a risk that those vehicles could be used to carry out one or more of the components related to trade based money laundering. Trade-based money laundering[41] is a method of ML that is believed to be prevalent internationally since verifying actual or purported trade movements and the identity of goods, shipments, documents etc. can be difficult. Criminals may also be attracted to use the IoM for the legitimacy that a British vehicle or address might convey. In response to this risk, Customs has issued Notice MAN 1000 on TBML.

High value assets such as property, yachts and aircraft are attractive to HNWI and PEPs some of whom may be seeking to invest the proceeds of corruption. Such assets may be purchased, sold and managed through IoM trusts and companies. In 2018 it was estimated that trusts and companies established in the IoM owned around 12% of the UK properties[42] owned by non-UK companies.

The misuse of vehicles to evade tax also features highly in international experience of TCSP risk and indeed this is reflected in SARs statistics where 50% of all SARs made by the TCSP sector are categorized as tax evasion being the underlying predicate offence.

TCSPs can also be vulnerable to TF risk. Examples of international typologies include:

[41] https://www.gov.im/media/1348726/notice-1000-man-trade-based-money-laundering-july-18.pdf

[42] BBC analysis, February 2018

- The operation of, or sending money to, charities or other NPOs that are actually front organisations;
- Companies which operate or run websites /social media accounts to distribute material supporting terrorism;
- Companies which are used to channel funds by more sophisticated groups;
- The exports of materials or natural resources e.g. historic artefacts, oil, diamonds, etc. to raise funds for terrorism.

No such TF cases have been identified within the IoM TCSP sector to date. It is important however for ML/TF purposes that TCSPs are aware of these risks and ensure that they have full CDD in place, including source of wealth. Seemingly superfluous complex structures and arrangements need to be treated with caution and any unusual activity concerning the trusts and/or companies being administered should be identified. The nature and activities of the business undertaken by the applicant seeking to establish and maintain a relationship with a TCSP needs to be well understood as does the nature and activities of the client companies and trusts, and the location of those activities.

Overall Risk

ML/TF risk can relate to misuse of TCSP services for the commission of the predicate offence, or for layering or integration of dishonestly obtained funds. There are existing and significant international typologies for the sector. The overall risk for ML is considered to be **Medium High** taking into account the threats and vulnerabilities, balanced against the controls in place in the sector; the overall risk for TF is **Medium**.

Convertible Virtual Currencies (CVCs)[43]

CVCs include crypto-currency e.g. Bitcoin and Ether. CVC's can be bought and sold through independent exchanges for fiat currency. For a currency to be convertible[44] a recognised third party market is required and that all that ownership rights can be transferred from one person to another (whether for consideration or not). CVCs can be used as a method of payment as an alternative to using fiat currency.

The registered CVC sector in the IoM consists of 28 businesses; it ranges from small CVC issuers to international CVC exchanges. Not all of these businesses have a physical presence in the IoM. The usage and purpose of each registered designated business is diverse and positioned within a rapidly evolving industry. The IoM has taken a proactive approach to mitigate risks through strengthening the designated businesses registration criteria in 2018. There is now, for example, a requirement for a CVC business to have (and continue to have) at least two resident directors and management and control of the business in the IoM. The IOMFSA has also targeted this sector as high priority for inspections. The sector is largely international based with non-domestic customers.

By way of a breakdown of activity in the IoM, the three key types of registered CVC's include the following simplified examples:

[43] Updated guidance from FATF adopts a new definition of 'virtual assets' and 'virtual asset providers' and clarifies that the FATF Standards apply to virtual-to-virtual and virtual-to-fiat transactions and to interactions involving virtual assets.
[44] The Designated Businesses (Registration and Oversight) Act 2015 provides a legal definition of CVC activity.

- **Administering, managing, lending, buying, selling, exchanging or otherwise trading** allows customers to exchange fiat currency for CVC and vice versa as well as trade between different CVC's.
- **Issuing, transmitting and transferring ("ICO")** a token or coin to raise funds for a particular product or software/service (typically blockchain). The token or coin purchased at the time of the ICO usually brings with it a benefit to the purchaser once the ICO is complete, for instance the token or coin is discounted at various times throughout the ICO (bigger discount early and for higher amounts purchased).
- **Providing safe custody or storage of CVC's** where customers can store or hold their tokens to pay for goods or services, typically referred to as a "wallet".

Seven of the businesses registered with the IOMFSA undertake all of these activities. The 2015 NRA noted that the expected growth in the sector had not happened to date and appeared to be adversely impacted by an inability to access banking services. Although there has been some growth in the sector this is relatively steady and securing banking facilities within Europe remains an issue. One of the reasons that businesses seek to register in the IoM may be that the credibility they gain by being located in a jurisdiction that has a well-established registration and oversight regime in respect of AML/CFT for CVCs. This in turn could help to secure banking services, however it is noted that it can be harder to obtain banking services for CVC businesses.

Since 2015, the IoM has required any person involved in the business of issuing, transmitting, transferring, providing safe custody or storage of, administering, managing, lending, buying, selling, exchanging or otherwise trading or intermediating CVCs , to be registered with the IOMFSA and overseen for compliance with the AML/CFT legislation. The Island is therefore among a small handful of countries that registers and supervises CVC businesses for AML/CFT purposes.

The IOMFSA oversees AML/CFT compliance for businesses that provide money service business style products in relation to convertible virtual currencies. The GSC regulates gambling activities relating to both convertible and non-convertible virtual currencies and has issued Practice Note GSC85 'Considerations for blockchain and virtual goods gambling'. Any CVC business acting in or from the IoM is captured under Schedule 4 of POCA and must meet the requirements of the AML/CFT Code 2019. The sector is subject to same AML/CFT obligations as all DNFBP license holders. The IOMFSA is responsible for oversight of the sector to ensure compliance with the Code, by virtue of the DBRO Act 2015. There are no entry qualifications required to work in the sector and no overall professional oversight body in the IoM for CVCs.

The IOMFSA publishes sector specific AML/CFT guidance notes concerning virtual currency businesses. The GSC has also published AML/CFT guidance for virtual currencies in respect of gambling. Guidance, which is currently being updated following the adoption of a new AML/CFT Code in 2019 will focus on the inherent risks of the sector and be updated in line with technological and regulatory developments.

The IOMFSA has conducted 8 inspections adopting a risk-based approach. Supervisory inspections have been focused to some degree on providing education to assist businesses in meeting their requirements although where serious deficiencies have been identified actions have been taken. SAR reporting increased moderately across the sector between March 2018 and June 2019.

Observations from IOMFSA inspections highlighted the ML/TF risk of the registered CVC not having a tangible presence in the IoM; this resulted in the IOMFSA updating its registration policy to include a minimum requirement that CVC businesses must have at least 2 resident directors and that management and control of the business must be in the IoM. This aims to enable the

IOMFSA to effectively undertake its statutory duty of overseeing the compliance of CVCs with AML/CFT legislation.

The IOMFSA continues to re-evaluate the IoM's oversight and other control environments to determine the most appropriate regulatory and supervisory regime for CVCs in consultation with key stakeholders. It has published guidance to inform the public about the nature of ICOs and the risks that should be considered before purchasing a token/coin. The IOMFSA has also issued guidance to persons seeking to launch an ICO in or from the IoM.

Of the audits carried out by the GSC on licenced operators using CVCs, it has been noted that these operators apply higher risk standards to their customers. For example, identity verification is applied earlier in the customer relationship than the standard regulations require, in addition to enhanced due diligence procedures being carried out earlier. This demonstrates the industry's awareness of the inherent risks associated with CVCs and its willingness to mitigate them.

Due to the increase in licenced gambling operators using ICOs to fund their business and use their unique token on their platform, the GSC has been required to reach out to CVC exchange providers in order to carry out specific audits on purchasers of ICOs to determine source of wealth and to rule out any potential use of proceeds of crime. The dialogue that has now opened up between the regulator and the exchange providers has been positive, with the exchanges granting the GSC additional knowledge, and the exchanges getting a better understanding of what is required from a regulator's perspective.

In 2017/18 the FIU received 15 SARs from the virtual currency sector. During 2018/19 the IoM had three identified cases relating to CVCs including one significant pan-European case which involved theft from online wallets held by domestic victims.

Vulnerabilities

The CVC sector is rapidly evolving; it is also complex, the level of regulatory (and investigatory) expertise in the field is limited and it is a challenge to keep up with developments. This inevitably leads to a degree of reliance on industry experts in the IoM as elsewhere, which brings its own advantages and disadvantages. The sector has some risks which are specific and some which are similar to those shared with other DNFBPs.

Identified risks include;

- Level of anonymity available which is greater than traditional non-cash methods and difficulty in linking an 'account' to a real identity;
- Non face-to-face business relationships; typically traded on the internet;
- May permit anonymous funding and anonymous transfers if sender and recipient are not adequately identified;
- The opaqueness of activities/transactions;
- Cross-border exposure;
- CVCs facilitate a wide range of financial activities and allow for quick movement of funds;
- High level of separation from the mainstream regulated financial sector;
- Non-centralised 'accounts' which can be opened without CDD checks;
- Potential use of anonymity software such as coin mixers and IP mixers;
- Difficulties in establishing source of funds and source of wealth;
- Quick and cheap global payments without ability to "chargeback";

- Lack of AML/CFT controls and clarity for CVC/VC compliance, oversight and enforcement in many jurisdictions where transactions are segmented across several countries;
- The rapidly evolving nature of CVC related technologies requires high-level specific knowledge and expertise within the regulatory sector which may potentially be lacking;
- The volatility of CVC values and limitation of availability may be problematic to CVC based businesses. Specifically for the gambling industry, this may be an issue when it comes to paying out winnings, the value of which having increased significantly from when a bet is first placed. Additionally, it is a requirement for the value of all player funds held on a gambling platform to be matched by the operator, which may be difficult to do should the value of a CVC significantly increase or the CVC become unavailable.

CVC providers should carefully consider features, products or services that potentially disguise transactions or hinder CDD and related measures. Particular focus should be given where service providers have links to many jurisdictions and/or where transactions are from or to higher risk jurisdictions. Issuing certain types of CVCs, in particular, but not exclusively, ICOs give rise to potential risks of ML and TF.

Overall Risk

The IOMFSA has been working closely with the sector in order to raise awareness of AML/CFT obligations and this work is continuing. In particular there is a strong cooperative relationship between the IoM authorities and CVC exchanges in the IoM. Nevertheless, despite the control measures in place there are specific ML and TF risks within the sector which, because of their nature, cannot easily be mitigated. The ECU has ongoing investigations concerning the sector. The ML risk for CVCs in the IoM is assessed as **Medium High** and the TF risk as **Medium.**

Estate Agents

Estate Agents in the IoM are involved in the buying, selling, renting and property management of residential and commercial properties. The sector is small and close-knit consisting in the main of well-established firms, although this has expanded slightly in recent years; there are 22 firms registered and Estate Agents make up around 6.6% of the total number of registered designated businesses.

The majority of the work undertaken is domestic; purchase of property and land outside of the IoM is most often dealt with by the TCSP sector, via property agents in the UK and elsewhere. National Income for Estate Agents in 2017/18 was estimated at less than £4.6 million which represents 0.1% of the Manx economy and is in line with data from the previous two years.

Estate Agents in the IoM are governed by the Estate Agent Act 1975. The Office of Fair Trading (OFT) is responsible for the registration of individual estate agents. Registration requires that an individual is a Fellow, Member or Associate of the Royal Institution of Chartered Surveyors (RICS) or Fellow of the National Association of Estate Agents (NAEA). Establishing an Estate Agency in the IoM requires a £100k bond to be secured plus their professional institution obligations[45]; currently such bonds are only available via one insurance company based in the Island. The IoM is unique in requiring degree level professional qualification and membership to practice since

[45] Requiring separate insurance for client monies.

1978; these additional professional obligations include redress schemes and professional conduct standards including anti-money laundering.

Funds (with the exception of rental payments) are not handled by Estate Agents; sale and purchase of property requires the involvement of Advocates who provide the conveyancing services and FIs[46], notably banks, all of whom are either registered or regulated for AML/CFT purposes. Estate Agents receive commission for securing the sale from the seller or a letting by the landlord, with sale payments largely being made from an Advocate's client account upon completion of the transaction. The majority of property lettings are residential face to face and of less than £1000 per calendar month.

The activities of Estate Agents are designated under Schedule 4 to POCA 2008 as undertaking business in the regulated sector. As such they are required to comply with the requirements of the AML/CFT Code. The activities of Estate Agents are also included in the DBRO Act 2015, giving the IOMFSA the power to oversee the sector in relation to AML/CFT compliance.

In 2018 5 disclosures were made to the FIU from the Estate Agency sector; all were of sufficient interest to be disseminated to a number of different locations. This represents a small but important increase in the level of SAR reporting which is reflective of an increasing level of awareness within the sector.

If a UK Estate Agent lists IoM property online for sale this falls outside the IoM DNFBP regime, and would rely on UK law. However AML/CFT checks by IoM conveyancing or bank transactions would provide AML assurance. Any money laundering offence would also be committed in the IoM due to the location of the property. The OFT ensures that any non-IoM Agents selling property in the IoM are notified of the requirement to register under the 1975 Act and as a DNFBP or to undertake arrangements with a registered IoM Agent.

Vulnerabilities

The purchase and selling of land and property to disguise the proceeds of crime and corruption is a significant typology internationally. Real estate is a relatively stable and safe investment which can be effective in generating returns or capital; it is therefore attractive to money launderers seeking to integrate or layer their assets.

Estate Agents do not handle the funds involved in property sales; this may lead to a risk of overreliance by Estate Agents on the role of conveyancing staff and an assumption that the responsibility for AML will rest predominantly with the Advocate firms.

Residential and commercial rentals, particularly non-local business, where rentals are offered to internationally-based individuals and companies, are a primary AML risk area; however this is likely to be a very low % of the business. Continuing business, where Estate Agents manage the property on behalf of the landlord and take possession of the rent on behalf of the landlord is common, but mostly with lower value rental properties. If an Estate Agent remains in this position they are required to complete customer risk assessments on the landlord and the tenant as well as ongoing monitoring. It is common for an Estate Agent to receive the full rental payment into their client account, deduct their management fees and expenses before sending the remaining funds to the landlord. The amounts are not normally high and are scrutinised due to commercial

[46] Conveyancing makes up a significant proportion of the domestic work undertaken by Advocates, see relevant section under Legal Services.

business needs; overall the real return on investment is small and unlikely to be an attractive option for ML.

Estate Agents dealing with the customer are well placed to identify unusual or suspicious behaviour. Suspicions and investigations have arisen in the past concerning cases where purchase of real estate in the IoM has been made using the proceeds of criminality. In 2019 the FIU published two typologies for the sector specific to the IoM, one concerning the provision of cash for a rental and the other concerning an individual from a higher risk jurisdiction looking to invest in property in the IoM.

Estate Agents in the IoM should be particularly aware of the following;

- Use of estate agency services to provide additional layers of legitimacy to criminal financial arrangements, especially involving large sums;
- Over or under-valuation of real estate - buying or selling property at a price above or below its market value;
- Successive sale or purchase of properties, especially large numbers of properties, with unusual profit margins especially involving purchases by apparently related participants;
- Uncertainty as to the true identity of the seller/purchaser; avoidance of personal contact.
- Purchasers resident in a high risk jurisdiction;
- Property which is offered for sale on behalf of a third party;
- Payment in cash in respect of leases and rentals managed through Estate Agents;
- Residential and commercial rentals for non-domestic clients;
- Lack of interest in the details of properties; anxiety to rush transactions through without any apparent concern regarding costs;
- Involvement of persons known to have convictions for, or who are publically known to be linked to acquisitive crimes, or where there are suspicions of involvement in activities that may be related to money laundering.

The IOMFSA has a risk based schedule of supervisory inspections in place. However, AML requirements are relatively new to the sector and, alongside monitoring, the IOMFSA and FIU are continuing to work to raise understanding, awareness and acceptance of the responsibilities and requirements that this entails and to arrange and deliver training programmes of AML/CFT.

Overall Risk

Awareness of AML/CFT requirements within the sector is increasing but ongoing work is required to improve AML knowledge and the effectiveness of compliance systems for AML and SAR reporting. The ML risk for Estate Agents in the IoM is assessed as **Medium Low**. This is because the sector is small and highly domestic in nature, the sector is not primarily cash based, there are a number of other financial and non-financial professionals engaged in the transactions and active oversight takes place. The TF risk for purchase of property in the IoM is regarded as **Low.**

Non-Profit Organisations (NPOs)

As of 2019 there are around 700 registered charities in the IoM; charities are required to register under the Charities Registration and Regulation Act 2019 (the Charities Act 2019) which replaced the Charities Registration Act 1989. The list of charities is publically available on-line via the Central Registry. Whilst the Central Registry holds the Charities Registry the regulation is

undertaken by the Attorney General's Office as the Attorney General has the role as de-facto guardian of the public under legislation.

A small number of charitable organisations send money abroad for emergency aid and for projects linked to the UN sustainable development goals; this presents a risk that legitimate funding might be used or diverted for criminality and/or to fund localised terrorist activities. Therefore, non-profit organisations with an annual or anticipated annual income of £5,000 or more, which have remitted or are anticipated to remit at least £2,000 in one financial year to one or more ultimate recipients in or from one or more higher risk jurisdictions and where the decision to remit the funds is made in the Island are defined in Schedule 4 to POCA as Specified Non-Profit Organisations (SNPOs).

SNPOs are required to comply with the Anti-Money Laundering and Countering the Financing of Terrorism (Specified Non-Profit Organisations) Code 2019 SNPO Code 2019) and register under the DBRO Act 2015. The IOMFSA conducts inspections to these SNPOs to ensure that they are complying with the requirements of the SNPO Code 2019.

The number of SNPOs in the IoM is at any given time very small. The broader charitable sector is predominantly domestically orientated, supporting small to medium sized local charities. There is no AML/CFT oversight of these charities (or non-charitable NPOs); however the checks undertaken by the Attorney General's Chambers at the point of registration, alongside increased investigatory powers under the new 2019 Charities Act, provide opportunities for any identified AML/CFT concerns regarding charities to be identified and reported.

There is no formal register for non-charitable NPOs; there is however sufficient open source material available to form a picture of the nature and activities of this sub-sector and consequently to assess the likely level of AML/CFT risk presented. Currently there is nothing adverse reported by the FIU in respect of IoM non-charitable NPOs and no contrary intelligence from other external sources; IoM NPOs have not figured in any reports or typologies either domestically or in those of other countries, there have been no MLARs received and to date no investigations into ML/TF concerning NPOs in the IoM.

Vulnerabilities

The main vulnerability globally identified in respect of NPOs and, in particular, for charities is TF. There are no examples of the use of NPOs in the IoM for ML or TF.

A number of factors make charities attractive to TF including sending money to or working in higher risk regions or regions bordering areas of conflict. Money collected may be knowingly used to fund illicit activity or misappropriated including, potentially, by partner organisations, for the purpose. Areas of legitimate work such as health and education can be subverted for other purposes and this can be difficult to establish. The level of knowledge and understanding of trustees for ML and TF can be variable, especially with smaller charities and NPOs.

Vulnerabilities evidenced by IOMFSA work with SNPOs include a need to improve the AML/CFT knowledge of the executive and non-executive members and improving the effectiveness of compliance systems. The IOMFSA and the FIU have conducted outreach and training to improve risk awareness of TF.

The MONEYVAL assessment identified that further work was required in relation to understanding potential TF risks, for example arising from financial activity of foreign NPOs and transfers of funds to high risk jurisdictions. This work is ongoing and is addressed with the TF Threat part of this NRA.

Overall Risk

The scope and size of the SNPO sector is extremely limited. There is a risk of lone actors seeking to abuse legitimate vehicles in order to raise money for terrorist purposes and this is recognised by the authorities. There is currently no evidence of the sector being abused for ML or TF and no intelligence to the contrary. The risk of an IoM NPO, including unregistered NPOs, being exploited by either insiders or outsiders is considered to be **Low** for ML and **Low** for terrorist financing.

Moneylenders

Moneylenders are covered by the Moneylenders Act 1991; they must register with the OFT which requires the disclosure of civil and disciplinary proceedings as well as offences and criminal matters by specified persons as part of the registration process to ensure applicants meet a 'fit and proper' test. The OFT maintains a register of persons carrying on a business of lending money in the IoM which is available for inspection. Anyone other than a bank or other exempt organisation who runs a business of lending money in the IoM must be registered with the OFT as must anyone who collects money on behalf of a lender**.**

The business of lending, unless exempt, is designated under Schedule 4 to POCA as undertaking business in the regulated sector. As such Moneylenders are required to comply with the requirements of the AML/CFT Code. The activities of this sector are also included in the DBRO Act 2015, giving the IOMFSA the power to oversee the sector in relation to AML/CFT compliance. Moneylenders conducting relevant business must register with the IOMFSA before they commence trading. Designated activities include (but are not limited to) the following:

- lending including, but not limited to, consumer credit, mortgage credit, factoring and the finance of commercial transactions in respect of products other than consumer products for and on behalf of customers;
- providing financial leasing arrangements in respect of products other than consumer products for and on behalf of customers;
- providing financial guarantees and commitments in respect of products other than consumer products for and on behalf of customers.

There are 55 businesses registered with the IOMFSA for conducting money lending.

Vulnerabilities

Moneylending in the IoM may present a number of different risks. At one end of the market, loans made available, typically to low earning customers, may present potential for the risk of laundering the proceeds of crime, as repayments are often paid in cash. Providing verification of the source of this cash can be difficult, leading to a risk of the laundering of, amongst other things, drug money. The risks are different for larger loans e.g. for cars and home improvements where there is more likely to be better monitoring and documentation, and at the upper end of the market where e.g. business to business lending may take place.

Typology reports indicate that the most common vulnerability faced by lenders is where cash is drawn down from the provider and then repaid with the proceeds of crime, either very quickly afterwards or over a short repayment period. This allows for the exchange of criminal

proceeds with clean money from the loan provider and provides the criminal with documented evidence of a seemingly legitimate source of funds. Early repayments carry a risk that the funds have emanated from a criminal lifestyle. Similarly early repayment of loans and then the taking out of another loan soon afterwards is also a recognised typology. Moneylenders in the IoM should be particularly aware of the following;

- Customers who are secretive or evasive e.g. about the source of funds, need for the loan or avoids personal contact.
- The use of agents or intermediaries with no apparent reason.
- Reluctance of customers to provide information.
- When false or misleading information is provided.
- Where customers are known to have convictions for acquisitive crime or to be associated with such persons.
- A frequent change of lender or where it is known that lending has been refused by another Moneylender.
- An absence of documentation.
- Where there are changes to instructions at the last minute.
- Customers who seem unconcerned with early repayment fees, additional charges etc.
- Where repayments are made by a person other than the one who took out the loan.
- Overpayment of loans.

While there is a recognised typology concerning lending being used to fund TF activities, e.g. where a customer secures a loan for TF-related purposes without, of course, the intention of paying it back, no such cases have been identified in the IoM.

Overall Risk

Although there are a comparatively large number of registered moneylending businesses in the IoM the volume and level of transactions dealt with are low compared to many other DNFBP sectors. The majority of customers are domestic with a sizeable proportion known to the lenders. There are no domestic typologies for ML or TF relating to moneylending in the IoM. The risk for ML is assessed as **Medium Low** and for TF as **Low**.

High Value Goods Dealers

The following businesses dealing in high value goods are present in the IoM;

- Car and Motor Cycle dealerships
- Dealers in jewellery and precious metals
- Auctioneers and antique dealers

Identifying the size of the High Value Goods sector is difficult, since it is not differentiated within GDP data and is included under 'generic retail' for tax information. However information collected from Government agencies and from open source material indicates that the sector is small, predominantly domestic and that overall turnover is relatively low, albeit that the assets sold may individually be valuable.

High Value Goods Dealers are subject to the requirements of Schedule 4 of POCA whenever a transaction involves accepting a total cash payment (or any structuring of a cash payment)

amounting to EURO 15,000 or more. The sector is also covered by the DBRO Act 2015, giving the IOMFSA power to oversee High Value Goods Dealers for AML/CFT purposes. If businesses accept cash payments of EURO 15,000 or more without being registered with the IOMFSA they commit an offence; the IOMFSA therefore recommends that clear company policies and procedures are adopted which prevent staff from accepting such transactions.

As of 2019 there are 2 businesses registered with the IOMFSA.

Vulnerabilities

Laundering money through the purchase and re-sale of high value goods is a well-recognised international typology. Payments by cash or similar monetary instruments create a higher risk for ML as there will be no clear audit trail and the origin of the funds is harder to trace. The high value goods themselves tend to be transportable, internationally exchangeable and easy to trade anonymously. Gold is particularly attractive to money launderers because it has a high intrinsic value, is readily accepted across the world and can be melted down into many different forms.

Where a customer seeks to make large payments using cash or similar monetary instruments and in particular where this is a frequent occurrence, the business should take care to examine the circumstances. If these do not stand up to scrutiny an internal disclosure should be made.

- Over-payment by a customer who then requests their over-payment is refunded by wire transfer or cheque instead of cash;
- Transactions that appear to be conducted on behalf of another person;
- Customers paying for goods in cash where previously they did not do so;
- Small denominations of cash used for a large payment;
- Sudden change, offering to pay by cash instead of using debit/credit card or cheque;
- Unusual delivery requests e.g. items shipped to a third party overseas;

Businesses are required to report relevant transactions to the IOMFSA at the end of the financial reporting year; therefore it could potentially be up to 12 months before the authorities are notified. It would be beneficial if businesses were required to make the report to the IOMFSA at the time of the transaction and this was sent to the FIU in a process similar to the Cash Declarations received from CED. Investigations could then be made at the time and any relevant interest actioned by local authorities in a timely manner.

Overall Risk

There are some vulnerabilities, particularly in terms of car and motorcycle dealerships due to the limited amount in the IoM that are UK or European franchised dealers (which are obligated to follow group policy regarding handling cash). Nevertheless High Value Goods Dealers represent a very small part of the DNFBP sector in the IoM and the indications are that the sector presents a **Low** risk nationally for ML and for TF.

8. Cash

Note that the following are addressed under Financial Services (6) 'Other Financial Institutions'

- Money transmission services: payment services directly and e-money providers

- Money transmission services: bureau de change, payment services as agent, cheque cashers
- Credit Unions
- Loan/Equity Crowdfunding

The use of cash by criminals at all stages of the ML process, and for TF purposes, is well-recognised. Cash can be used to disguise the origin of criminal proceeds, because it is difficult to trace and therefore link to criminality. It may also be the product of illicit activities, in the IoM from the trafficking of drugs into the Island for example. Cash smuggling is a significant threat throughout Europe and, since cash is generally used for low-value payments, the continued international demand for high denomination banknotes e.g. the EURO 500 note, is suspected of being linked to criminality.

The MONEYVAL report of 2016 expressed some concern regarding the controls placed on cash by the IoM and recommended a review and further improvements at the border for the identification of non-declared or falsely declared cash. The report also noted that the 2015 UK NRA identified cash-couriering as a high risk and that this could impact on the risk faced by the IoM, since there were no borders and cash could be freely transported between the UK and the IoM.

The authorities have taken a number of actions since the mutual evaluation took place which include;

- Improved domestic cooperation, in particular the establishment of a formal operational mechanism between authorities, evidenced via seizures (and forfeiture) of cash and vehicles involved in cash and drugs smuggling.
- New legislation broadening the powers of CED to allow targeted action or controls on goods, cash etc. entering or leaving the IoM.
- Efforts at increasing awareness of reporting requirements on cash movements to passengers.

Cash controls and borders have also been reassessed for this NRA. That assessment confirms that the IoM has a very highly formalised economy, which is post-industrial and financial services based. The black economy is correspondingly small and limited to the sale of illegal narcotics and cash-in-hand manual work, with the greater volume of financial transactions taking place through the recorded financial system.

The assessment was informed by the amount of IoM cash in circulation including the amount repatriated from the UK to the Island each month (since Manx currency, whilst being sterling, is not freely negotiable in the UK or elsewhere). Furthermore, the vast bulk of economic activity in the IoM requires VAT registration and licensing by one or more authorities, which formalises most activity.

The conclusions are that, since the IoM is not a cash-based society, any large cash deposits into the banking sector or via other routes would raise suspicions resulting in an SAR. The controls in place could not prevent cash being brought into the IoM and integrated into the financial system in small amounts; however there is an obligation to report *any amount* that is suspicious. In respect of investing in assets, there are limited opportunities to exchange significant amounts of cash for high value goods and all relevant sectors are covered by AML/CFT reporting requirements.

The authorities have also considered any impact on risk as a consequence of the cash-couriering risks identified by the UK and conclude that the risks are substantially different. The UK is a hub for international travel and commerce with direct links across the globe, by air, sea and rail and substantial established populations from across the world. This volume of travel, diversity, opportunities for transacting in cash, and other relevant factors acknowledged by the UK, do not equate to the situation in the IoM.

The assessment identified areas where further improvements need to be delivered;

- Better sharing with the FIU of intelligence obtained at the ports;
- Continued emphasis on coordination between agencies and in respect of cash seizures generally;
- A focus on the illicit movement of cash leaving the IoM suspected of being linked to drug dealing and organised crime;
- Further training and awareness with port security staff and with courier services (which are increasingly used for bringing goods into and out of the IoM).

The purpose of border controls is to supervise the movement of goods and people, and since these areas are incorporated into long-standing agreements concerning a common customs arrangement and a Common Travel Area, significant 'border' resources for the IoM seaports and airport have not been necessary. Given the anticipated change of status of the UK with the EU however, this is an area which is requiring ongoing and active review of risk in relation to cash controls.

9. Legal Persons and Legal Arrangements

The 2016 MONEYVAL assessment acknowledged that "the extent to which legal persons and legal arrangements can generally be misused for ML/TF purposes is well understood." However the assessment recommended that an exercise should be conducted by the IoM authorities "to specifically consider how legal persons and legal arrangements established under Isle of Man legislation have been used to disguise ownership or to launder the proceeds of crime."[47] The 2015 NRA assessed risk in relation to the TCSP sector but did not include a broader review of companies and legal structures such as partnerships with a legal personality[48].

Consequently in 2017 and 2018 the FIU led a multi-agency working group which reviewed relevant data and information (for example concerning disclosures to the FIU, requests for MLA and cases referred to CED), relating to evidence of the misuse of legal persons and arrangements for laundering the proceeds of crime.

IoM companies and IoM TCSPs made up the majority of relevant disclosures that were analysed; foundations, industrial societies, limited liability companies and limited partnerships made up only 1% of the Companies Registry and therefore perhaps unsurprisingly did not feature. A (small) majority of the legal entities identified were 1931 Act Companies, closely followed by foreign companies administered and regulated in the IoM but incorporated elsewhere, 2006 Act companies and finally trusts governed under IoM law.

[47]Anti-money laundering and counter-terrorist financing measures: Isle of Man Fifth Round Mutual Evaluation Report. MONEYVAL December 2016 (paragraph 39).
[48] General partnerships do not have a legal personality and are therefore not included.

No features of legal persons and arrangements established under Manx legislation were identified which make them particularly susceptible to abuse. The use of companies and trusts for suspected tax evasion featured highly within the relevant disclosures reviewed, as did the use of those entities for fraud, being part of complex structures used to facilitate money laundering in several jurisdictions. These findings accord with the 2015 NRA which concluded that tax evasion and fraud are the most likely international money laundering threats to the IoM.

The work of the multi-agency group, coordinated by the FIU, is continuing and consideration is being given to other identified and emerging areas of activity that present a potential threat.

Central (Companies) Registry

The Central Registry (part of the Department for Enterprise) is responsible for keeping registers of companies, foundations and limited partnerships, all of which are publically available and a register of the beneficial ownership of companies, which is available to law enforcement and competent authorities for permitted purposes. There is no register of trusts in the IoM. In November 2018 a total of 26,501 corporate and legal entities were registered, including 1931 Act companies, 2006 Act companies, Foundations, Limited Liability Companies and Limited Partnerships with legal personality.

The Companies Registry is a member of the European Business Registry Association (EBRA)[49], and two of its working groups – (I) the Beneficial Ownership working group, and (II) the Company Law Package working group.

The Companies Registry monitors compliance with the statutory filing obligations under the relevant Acts with a focus on the timely filing of information to ensure that the registers are accurate and up to date. The Companies Registry performs a strike-off against legal entities which fail to submit annual returns, maintain a valid registered office or fail to have a registered agent. Following the introduction of the Anti-Money Laundering and Other Financial Crime (Miscellaneous Amendments) Act 2018, Companies Registry has the vires to make enquiries as it considers appropriate to establish the accuracy of information submitted for registration under the relevant Acts, however Companies Registry is not responsible for monitoring compliance in respect of the Beneficial Ownership database. Companies Registry checks and files the information submitted for the database however the IOMFSA undertakes the supervisory function and, where required, an enforcement role.

Preventive Measures

In order to manage and reduce the risk of companies and trusts being misused for ML or TF the IoM treats TCSPs in the same manner as FIs. Corporate Service Providers have been regulated since 2000 and licencing was extended to include the regulation of Trust Service Providers in 2005. The IOMFSA is responsible for the licencing and supervision of TCSPs; Chapter 7 provides further details.

The Anti-Money Laundering and Countering the Financing of Terrorism Code 2019 (AML/CFT Code 2019) ensures that information is available to the authorities. Section 35 of the AML/CFT

[49] The EBRA was established in 2019 by the merger of the European Business Registers and the European Commercial Registers' Forum. Before the merge the Registry was a member of the European Commercial Registers' Forum.

Code 2019 requires that a relevant person (someone carrying out business in the regulated sector) must keep all records required by the Code in the following manner:-

(a) If the records are in the form of hard copies kept in the IOM, they must be capable of retrieval without undue delay;
(b) If the records are in the form of hard copies kept outside the Island they must be made available within the Island within 7 working days;
(c) If the records are not in the form of hard copies (such as records maintained on a computer system) they must be readily accessible in or from the Island and capable of retrieval without undue delay.

Bearer shares do not present a risk in the IoM as they are prohibited under the Companies Acts 1931 to 2004 and the Companies Act 2006. It is an offence to issue, convert or exchange bearer shares under these Acts. Since the last NRA the IoM has introduced further relevant preventive measures which include the following;

In 2018 the Anti-Money Laundering and Countering the Financing of Terrorism (Unregulated Trustees) Code was introduced, bringing non-professional domestic trustees and foreign trustees under the same record-keeping requirements as professional trustees.

The AML/CFT Code 2019 introduces additional requirements concerning introduced business to ensure that the identity of the customer is known. If more than one third party from outside the IoM is involved, then the customer's identity must be verified using documents obtained either directly from the customer; from the introducer (if they were obtained from the customer or a third party who has met the customer); or from a third party who has met the customer. These measures are in addition to a requirement to conduct a risk assessment and to undertake enhanced due diligence if the customer is higher risk.

IoM Incorporated Companies and Foreign Companies

1931 Act Companies: Companies incorporated under the Companies Acts 1931-2004 are subject to a traditional English company law regime. Every 1931 Act Company must have at least two individual directors. Corporate directors are not permitted. There is no requirement that the directors of a 1931 Act Company must be resident in the IoM. Often tax considerations will dictate where directors of the company are resident. Provision for appointment of directors is usually made in the company's articles of association and the management of the company is usually vested in the board of directors collectively. Every 1931 Act Company must at all times have a registered office in the IoM and is required to file an annual return at the Companies Registry.

2006 Act Companies: The Isle of Man Companies Act 2006 (the Act) came into force on 1 November 2006 and introduced a simplified corporate vehicle into IoM law. Unlike a 1931 Act Company, a 2006 Act Company is permitted to have a single director which may be an individual or a body corporate, appointed within one month of incorporation. A 2006 Act Company can voluntarily elect to file a copy of its register of directors and/or register of members with the Registrar. The responsibilities of the director include managing the company in accordance with the provisions of the Articles of Association, to ensure compliance with the Companies Acts and filing information with the Registry. A 2006 Company must have a single member (individual or corporate) stated on the Memorandum and have a Registered Agent in the IoM.

Foreign Companies: A company incorporated in a jurisdiction outside of the IoM and which establishes a place of business or that owns or rents land in the IoM, must register as a foreign company under the Foreign Companies Act 2014. Registration documents must be delivered to

the Companies Registry within one month of the establishment of the place of business or the acquisition of the land; a foreign company that fails to register, together with its officers, commits an offence. The interpretation placed upon what is meant by 'establishing a place of business' means, unless real estate is involved, that many companies which are administered in the IoM and incorporated abroad, are not entered onto the 'F-register'. This is not necessarily considered to create a ML risk to the IoM but does create potential reputational issues.

Partnerships (including Limited Partnerships and Limited Liability Companies)

There are two types of partnership under IoM law; General Partnerships, which do not have a separate legal personality and therefore cannot own assets or enter into legal arrangements in their own right. Any assets are held jointly by the partners and they are mainly used domestically by individuals undertaking local trading activity. There are also Limited Partnerships, which may elect to have a legal personality. In such case, the partnership has the ability to own assets in its own right but remains tax transparent.

In addition, the IoM law also provides for the formation of Limited Liability Companies (LLCs) which are treated in all respects as partnerships. An LLC is not legally a partnership, but it is treated as a partnership for income tax purposes. It has legal personality and can own assets in its own right but is transparent for tax purposes.

Foundations

Foundations were introduced into Manx law by the Foundations Act 2011. An IoM foundation has its own separate legal personality although, unlike a company, it does not have shareholders. Every foundation is required to have a registered agent which is the holder of a Class 4 licence issued by the IOMFSA under the FSA08. Upon successful application, the Registrar enters the details of the foundation into its register together with the foundation instrument. The register is available for public inspection on payment of a fee. A copy of the foundation rules must also be lodged with the registrar. Once established, a foundation acts through its council which will administer the assets of the foundation and carry out its objects in accordance with the foundation instrument and its rules. The council members perform much the same role as trustees or directors and the council must have at least one member. Foundations are required to submit an annual return to the Registrar and to pay an annual fee.

Trusts

IoM trust law is based on common law principles, supplemented and enhanced by legislation which, for the most part, mirrors its English equivalents. A Manx trust is not a legal entity; all the business of the trust is carried on by and in the name of the trustees. The IOMFSA regulates the activities of all persons providing trustee and other trust-related services by way of business in the IoM and requires them to hold a financial services licence issued under the FSA08 to undertake "Class 5" activities. Although there are no capital gains, inheritance, gift or estate taxes in the IoM trustees may be income tax payers and therefore obliged to file tax returns when they are resident in the IoM. Manx trusts with Manx resident beneficiaries are subject to income tax at 20% on undistributed income.

10. Beneficial ownership of companies, limited partnerships and foundations

The Beneficial Ownership Act 2017 repealed the Companies (Beneficial Ownership) Act 2012 and places all IoM corporate and legal entities under the same legislation regarding beneficial ownership. It created a central database for the recording of beneficial ownership of legal persons. The central database went live on 1 July 2017; guidance is issued by the IOMFSA.

In November 2019 there were 28,948 beneficial owners registered in relation to 19,136 live entities, the largest number of which (63%) were for 1931 Act companies.

Section 4(1) of the Beneficial Ownership Act 2017 ("the Act") defines "beneficial owner" as:-

"a natural person who ultimately owns or controls a legal entity to which this Act applies, in whole or in part, through direct or indirect ownership or control of shares or voting rights or other ownership interest in that entity, or who exercises control via other means, and "beneficial ownership" is to be construed accordingly".

The Act further provides that joint owners or controllers of an interest are each to be treated as beneficial owners, and that beneficial ownership may be traced through any number of persons or arrangements of any description. A registrable beneficial owner is defined as one who owns or controls more than 25% of the beneficial ownership of a legal entity to which the Act applies.

Beneficial Ownership information is held electronically by the DfE in a secure environment against the individual record of each legal entity. The Department is required by law to retain all information for between 10 and 12 years after a legal entity is dissolved or struck off.

The Act confers oversight functions on the IOMFSA; over their lifetime, relevant entities are searched by areas of identified risk. An entity may receive more than one inspection if deemed necessary. During inspections the information on the Database is checked against the information held by the relevant person. They will also be assessed for compliance with the other aspects of the Act.

Under section 26 of the Act, the Database is accessible by the following persons or bodies for the following reasons:-

(i) the Financial Intelligence Unit ("the FIU"), for the permitted purpose;
(ii) the Attorney General, for the permitted purpose;
(iii) the Assessor of Income Tax, for the permitted purpose;
(iv) the FSA, for the permitted purpose;
(v) the Chief Constable, for the permitted purpose;
(vi) the Collector of Customs and Excise, for the permitted purpose;
(vii) the Department for Enterprise, for the purpose of their functions under the Act;
(viii) the Gambling Supervision Commission, for the purpose of their functions under any enactment;
(ix) the Government Technology Services Division of the Cabinet Office, for the purpose of maintaining the Database and required website;
(x) a legal entity to which this Act applies, for the purpose of accessing the beneficial ownership information on the Database in relation to that entity; and

(xi) a third party authorised by a legal entity to which this Act applies, for the purpose of accessing the beneficial ownership information on the Database in relation to that entity.

The Act permits the FIU to disclose information obtained from the Database or from a nominated officer to an external intelligence or law enforcement agency. "External intelligence or law enforcement agency" is defined as a person or body engaged in a country which is a party to a beneficial ownership information sharing agreement (currently only the UK) and is named, referred to or contemplated in that agreement as a body to whom beneficial ownership information may be disclosed.

In April 2016, the IoM signed an Exchange of Notes (EoN) with the UK Government regarding the sharing of beneficial ownership information. Information is available to relevant law enforcement and can be exchanged within 24 hours with the UK or within one hour where urgent, for example if there are terrorist financing concerns. The IoM contributed to the 18 month UK 'Statutory review of the implementation of the exchange of notes on beneficial ownership between the United Kingdom, Crown Dependencies and Overseas Territories' which was published in June 2019. The review concluded that the EoN was extremely useful to UK law enforcement agencies; all enquiries made by the UK to the IoM were dealt with within the agreed timescales.

Public registers of beneficial ownership of companies

In December 2018, in response to concerns raised by the EU Code of Conduct Group on Business Taxation, the IoM introduced the Income Tax (Substance Requirements) Order. The EU Code of Conduct Group had concerns regarding a perceived lack of substance requirements that might result in profits being registered in the IoM without the commensurate economic activity taking place in the Island. The Order introduced a substance test for certain IoM resident companies that are within relevant business sectors. Those companies engaged in certain activities are required, when filing their income tax returns to report additional information to establish that they have adequate substance in the IoM for example number of qualified employees; operating expenditure and physical presence.

A political commitment was also made by the IoM regarding the sharing of beneficial ownership information with EU Member States. This will see the IoM work with the EU in the development of interconnected registry systems, as outlined in the Commission Implementing Regulation (EU) 2015/884 of 8 June 2015, with the aim of providing reciprocal access to law enforcement and tax authorities of beneficial ownership information.

Although the measures that the IoM has in place exceed current FATF requirements, the Island has continued to monitor international developments. With the emerging development of consensus at European and increasingly at international level, in June 2019, the IoM joined the other Crown Dependencies in making the following public commitment in line with the principles of the EU fifth Money Laundering Directive:

a) During 2021, to work collaboratively with the EU on the interconnection of the Islands' central registers of the beneficial ownership of companies with the registers in the EU. This is part of existing political commitments made by each of us to the EU to ensure that, on a reciprocal basis, legal and beneficial ownership information can be shared with EU designated competent authorities and Financial Intelligence Units (FIUs).

b) To enable access to our central registers of beneficial ownership of companies to obliged entities for due diligence purposes as soon as reasonably practicable following this interconnection referenced in (a) above and, in any event, before the end of 2022.

c) The EU is due to publish an Implementation Review of the 5th AMLD in January 2022. Within 12 months of that publication, we will each bring forward to our own parliament legislative proposals to establish public access to beneficial ownership data of companies held on a central register, in line with the principles of the EU's 5th AMLD.

In order to develop and implement the legislation referenced in (c) above, we will be informed by global best practice including the progress being made in EU Member States to introduce processes to verify, vet and regulate trust and company service providers and the submission of beneficial ownership information.

The IoM will be working closely with the other Crown Dependencies and with other key stakeholders including industry, on the next steps towards delivering an effective public register and continuing conversations with the EU to take forward the existing commitment to work with them as interconnected registers are developed.

Appendix 1 Geographic, Economic and Political Environment

The IoM is located in the centre of the Irish Sea, equidistant from England, Scotland, Wales and Northern Ireland. It has an area of 221 square miles (572 square kilometres). The resident population of the IoM in 2016 was 83,314. Demographically the 2016 census shows that nearly 50% of the Island's population are Manx-born and around 40% were born in the UK or Channel Islands. Small numbers of other nationalities are present from within Europe (5%) and from outside Europe (5%).

The IoM is a self-governing British Crown Dependency with HM Queen Elizabeth II as Head of State. It has its own government and laws, and a parliament, Tynwald, recognised as the oldest continuous parliament in the world. The UK Government, on behalf of the Crown, is ultimately responsible for the Island's defence and international relations. In recent years the IoM has – in agreement with the UK and its international partners – represented its own interests internationally, notably by concluding a significant number of bilateral tax agreements.

The Island has its own legal system and jurisprudence. English law is not directly applicable in general, but the Manx legal system is based on the principles of English common law and is accordingly very similar to English law in areas such as crime, contract, tort and family law. However, in certain areas, although modelled on English law, Manx law has adapted to meet the Island's own special circumstances, particularly with regard to direct taxation, company law and financial supervision. The Island's High Court judges hold the ancient office of Deemster and have jurisdiction over all criminal and civil matters.

The United Nations Convention against Corruption (2003) was extended to the IoM in 2009 and in 2012 the Palermo Convention against Transnational Organised Crime (2000) was also extended to the Island. Other relevant conventions which apply to the IoM include the Terrorist Financing Convention (International Convention for the Suppression of the Financing of Terrorism 1999) and the Vienna Convention (United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances 1988). The Island continues to pursue a legislative programme to ensure compliance with various international instruments targeting crime, terrorism funding, and international sanctions regimes.

There are limited customs barriers between the IoM and its closest neighbours and no fixed border controls to check the movement of people. This is a consequence of the Island's constitutional status as a Crown Dependency of the British Crown, the establishment in law of the Common Travel Area (CTA) which protects free movement between the UK, the Republic of Ireland and the Crown Dependencies and the customs union between the Island and the UK under the Customs and Excise Agreement 1979. There is free movement of passengers and freight between the UK and the IoM.

The IoM is financially autonomous and receives no financial assistance from either the UK or the European Union. The IoM is not represented in the UK or European Parliaments. Industries such as farming, fishing and tourism, which were the mainstay of the Island's economy, have since the 1970s onwards been joined by sectors such as financial services, e-business, shipping, aviation and high-tech manufacturing to create a diverse economy with an international base.

Domestically the IoM is one of the safest jurisdictions in the British Isles; overall the population is predominantly law-abiding which can be demonstrated from consistently low crime statistics and other sources of information such as levels of domestic tax compliance. In 2018-19 a total of 2503 crimes were recorded which was an increase of 10% over the previous year. The rise was

predominantly due to increases in recording of drug offences, fraud offences and assaults. The detection rate remains very high at 49.6%, an increase of 2.4% over the previous year.

The GDP of the IoM in 2017/18 was £5.26 billion. Financial and professional services account for 31.5% of national income. At the end of 2018 the Island's banking, insurance, pensions and securities sectors together held £146.2 billion in assets.

The Global Financial Centres Index 2019 ranks the IoM in size as 89th out of 104 IFCs. The Island accounts for 0.09% of the global market for offshore financial services according to the 2018 'Financial Secrecy Index' published by the Tax Justice Network, making it, in their classification, a 'small player'. The same index ranks the IoM as 42nd out of 112 countries, where one (1) equals the greatest secrecy; the 2015 NRA noted that the IoM was then ranked as 34th in that index. In a 2018 survey by the Financial Conduct Authority, UK regulated firms assessed the IoM as being in the lowest risk quartile in an assessment of financial crime risk (ranked 182 of 228 with 1 being the highest risk ranking)[50].

The relationship of the IoM with the EU is set out in Protocol 3 to the UK's Act of Accession (1972), and allows for free trade in agricultural and manufactured products between the Island and the EU. In all other matters, including direct tax and financial services, the IoM is in the position of a "third country" or non-Member State. However, due to the existence of the Customs and Excise Agreement with the UK, the Island is also recognised as an integral part of the EU fiscal (VAT and excise duty) territory. This position will change when the UK leaves the EU in2020.

[50] Financial Conduct Authority – Financial crime: analysis of firms' data, November 2018

Appendix 2 Legal and Regulatory Framework

The FATF sets the global standards for combating ML and TF and proliferation financing (PF) which are the 40 Recommendations and monitors their implementation via a peer review process. The IoM is not a FATF member in its own right, but participates in peer reviews and other activities through MONEYVAL, the European FATF style regional body.

The IoM is not a member of the EU and therefore EU money laundering directives, which require implementation of FATF Recommendations and other AML/CFT measures, into the laws of member states, do not apply. The Island does however give consideration to directives and will implement legislation as required, for example, measures concerning wire transfers.

Money Laundering and Terrorist Financing Legislation

The Proceeds of Crime Act 2008 (POCA) is the key piece of primary Manx legislation relating to money laundering. Amongst other things the Act is described as AN ACT to allow the recovery of property which is or represents property obtained through unlawful conduct or which is intended to be used in unlawful conduct; to provide for confiscation orders in relation to persons who benefit from criminal conduct and for restraint orders to prohibit dealing with property; to make provision about money laundering; to make provision about investigations relating to benefit from criminal conduct or to property which is or represents property obtained through unlawful conduct or to money laundering; to make provision concerning the importation and exportation of cash; to make provision to give effect to overseas requests and orders made where property is found or believed to be obtained through criminal conduct; to make provision for hearing evidence through television or telephone links, for obtaining evidence for use outside the Island and for the transfer of prisoners to assist in investigations; to make miscellaneous modifications to certain enactments; and for connected purposes. For terrorist financing the Anti-Terrorism and Crime Act 2003 defines proscribed organisations, provides a legal definition of terrorist property, sets out offences and forfeiture of property, notification requirements, terrorist investigations and counter-terrorist powers and offences concerning weapons of mass destruction.

The two key pieces of legislation relating to TF in Manx legislation are the Anti-Terrorism and Crime Act 2003 (ATCA) and the Terrorism and Other Crime (Financial Restrictions) Act 2014 (TOCFRA). Amongst a wide range of other matters, ATCA provides powers to proscribe organisations, creates offences for supporting and funding terrorist organisations, including facilitating funding and financing travel, defines terrorist property, creates offences for failure to disclose for the regulated sector, and provides for forfeiture of terrorist cash and property. TOCFRA provides for the giving of directions in respect of financing of proliferation or terrorism or money laundering, the freezing of terrorist assets, sets out disclosure requirements, offences for failure to comply with directions, designations and freezing orders. Both Acts have been subject to recent amendments to ensure that they reflect the latest FATF Recommendations as these evolve

Section 157 of POCA and Section 68 of the Terrorism and Other Crime (Financial Restrictions) Act 2014 also provide for Codes to be made; these are regulations which set out AML/CFT requirements for businesses. There has recently been significant revision and updating to these regulations and, as a result, there are a number of Codes in force;

- The Anti-Money Laundering and Countering the Financing of Terrorism Code 2019 (the AML Code)

- The Anti-Money Laundering and Countering the Financing of Terrorism (Gambling Sector) Code 2019 (Gambling Code)[51]
- The Anti-Money Laundering and Countering the Financing of Terrorism (Specified Non-Profit Organisations) Code 2019 (SNPO Code)[52]

The need for a civil penalty regime was highlighted in the 2015 NRA. Civil Penalty regulations were introduced in 2019 at the same time as the new Codes. The AML/CFT Code requires every relevant business to conduct CDD on a risk based approach, including;

- Enhanced Due Diligence (EDD) in high risk scenarios;
- Having an MLRO;
- Maintaining appropriate procedures and controls to deal with PEPs;
- Conducting ongoing maintaining of business relationships;
- Keeping adequate records; and
- Having effective staff training in this area.

The definition of businesses caught by the AML/CFT Code goes much wider than financial services and also includes; issuers of Virtual Currencies, Estate Agents and Accountants amongst others.

The SNPO Code is shorter than the AML Code and specifically targeted to the risks of this sector in the IoM. The Gambling Code covers both online and terrestrial gambling. Civil penalties for gambling were introduced in 2018.

Both regulators also issue guidance to industry (including in the case of the IOMFSA sector-specific guidance) for various purposes including illustrating best practice, to assist relevant persons in complying with legislation and to provide examples or illustrations. Guidance is not law, however it is persuasive. Where a person follows guidance this would tend to indicate compliance with the legislative provisions, and vice versa.

International Sanctions

The IoM Government is strongly committed to fulfilling its international obligations with regard to:

- sanctions regimes, and denying terrorist groups access to the financial system;
- countering the proliferation of weapons of mass destruction; and
- effective controls on the export and trade in military equipment, dual-use items, and other goods of concern.

Persons and organisations believed to be responsible for, or implicated in terrorist activities or the funding of such activities, are the subject of asset freezing measures introduced by various United Nations Security Council Resolutions (UNSCRs) and European Union (EU) regulations. The requirements placed on the IoM by these measures are implemented domestically by the Terrorism and Other Crime (Financial Restrictions) Act 2014 (TOCFRA). The Act also allows the Treasury to impose freezing orders or to issue directions to persons and businesses in the regulated sector requiring them to limit or cease business with named persons, entities or

[51] This Code replaces the Online Gambling Code 2013
[52] SNPOs were previously covered by the AML/CFT Code 2015

territories, or require enhanced customer due diligence, systematic reporting or ongoing monitoring. Changes made to legislation in 2016[53] ensure that UN listings can be implemented in the IoM without delay.

It is the policy of the Isle of Man Government to maintain implementation of international sanctions measures in line with such measures as have effect in the United Kingdom from time to time. The law and procedures dealing with the export of military or other goods of concern and technology or dual-use items, or trafficking or brokering in such things, also correspond to those in place in the UK.

The lead agency with regard to trade and financial sanctions within the Island, and for export and trade controls and licensing, is the Customs and Excise Division of the Treasury (CED). CED publishes Public Notices explaining the sanctions and export and trade controls that are in force.

Industry Supervision

The IOMFSA is responsible for regulating and supervising licenced FIs undertaking regulated activities and for registering and oversight of DNFBPs for AML/CFT purposes. The IOMFSA will conduct investigations into any potential liability arising from breach of AML/CFT legislation by persons undertaking regulated activities. The GSC licences and regulates all gambling activities, including online gaming, which is a significant sector in the IoM and will also conduct investigations into potential AML/CFT failings where required.

The IOMFSA will not issue a licence for deposit taking, investment businesses, collective investment schemes, corporate and trust services, money transmission services or 'any financial service or financial activity of a specified kind carried on by a person of a specified description', unless the applicant meets certain requirements and is managed and controlled in the IoM (FSA08). Similar provisions apply under the Insurance Act 2008.

The Licensing Policy for Regulated Activities made under the FSA08 specifies at (2.8.1) that "It is a fundamental requirement that a licence holder should not be a mere shell; an applicant must establish a real presence in the IoM …". A branch of a company incorporated in another jurisdiction must demonstrate real presence by registering as a foreign company that has established a place of business in the Isle of Man and there should be 2 or 3 IoM resident officers (2.8.4).

Certain roles must be in place (the holders of which must also must be fit and proper), for example, directors, a compliance officer, a money laundering reporting officer, etc. Qualitative requirements relating to staff are laid out in the IOMFSA Training and Competence Framework guidance (dated July 2017) according to the different roles held.

The IOMFSA has the power to issue discretionary civil penalties[54] in respect of a serious regulatory failing, such as deficiencies in the entity's corporate governance, systems and internal controls, or fitness and propriety of any of the entity's directors, controllers or key persons. In June 2019 the IOMFSA also obtained the power to issue civil penalties for AML/CFT failings. The GSC has the power to inspect its licensees in respect of all areas of status and conduct, and conducts regular audits of its licensees. Where an operator fails deliberately to meet the requirements the GSC would revoke the licence on the ground of unfit and improper control of the licence. The GSC has

[53] Terrorism and Other Crime (Financial Restrictions) Act 2014
[54] Under the FSA2008 and under the Insurance Act 2008

had a civil penalty regime for AML/CFT failings since January 2018 and has issued guidance to accompany this.

Further details on the preventive and supervisory measures taken by the regulators can be found under the relevant financial and non-financial sector in Chapters 6 and 7.

Law Enforcement

The Economic Crime Unit (ECU) is responsible for investigating cases of money laundering, terrorist financing and other financial crime. The ECU is a specialist unit within the police (IoM Constabulary) and is led by the Detective Superintendent, Head of Financial and Cybercrime.

The Financial Intelligence Unit (FIU) is the national centre for the receipt and analysis of suspicious transaction reports and other information relevant to money laundering, terrorist financing and financial crime and for the dissemination of information resulting from that analysis. The FIU is an independent Unit with its own Board and is led by the Director, FIU.

The ICART is a Directorate of the Attorney General's Chambers. ICART includes the Asset Recovery Unit (ARU) which identifies, restrains and recovers criminal assets in the IoM. ICART, on behalf of HM Attorney General, has conduct of all MLARs made by, and sent to, other jurisdictions in relation to criminal investigations and prosecutions including obtaining evidence, restraining assets in the IoM and enforcing confiscation orders. ICART operates under the superintendence of HM Solicitor General.

The Prosecutions Division of the Attorney General's Chambers, under the guidance of the Director of Prosecutions, prosecutes on behalf of HM Attorney General, all criminal offences in the IoM including money laundering and other financial crime.

The Customs & Excise Division (CED) is a division of the Treasury Department. CED is responsible for the administration of UN and EU financial and economic sanctions and export licensing controls in the IoM.

The Income Tax Division (ITD) is a division of the Treasury Department. ITD is responsible amongst other things for dealing with exchange of tax information requests at both a domestic and international level and all international matters affecting direct taxation, including liaison with the EU and OECD and negotiation of Tax Information Exchange Agreements (TIEAs) and Double Taxation agreements (DTAs).

Tax Transparency

The Island has a transparent tax code; there are no banking secrecy laws. Between 2005 and 2015 the IoM automatically exchanged information on savings income with 28 EU Member States under Directive 2003/48/EEC of the Council of the European Union.

Further measures have been successfully implemented to deliver tax transparency which include:

- since 2014, automatic exchange of financial account information with the United States Internal Revenue Service in accordance with the FATCA arrangements;

- automatic exchange of financial account information with HM Revenue and Customs in accordance with a FATCA-style Intergovernmental Agreement in respect of financial account information in the 2014 and 2015 calendar years;
- since 2016, automatic exchange of financial account information with all jurisdictions that have committed to, and fully implemented, the OECD Common Reporting Standard;
- since 2016, a move to amend existing Double Taxation Agreements ('DTAs') and mini-DTAs to include measures that are in line with the Island's commitment to the OECD's Base Erosion and Profit Shifting ('BEPS') initiative. These include, for example, measures preventing abuse of treaties through 'treaty shopping';
- since 2017 (and including 2016 on a voluntary basis), automatic exchange of Country by Country Reports, in line with the Island's commitment to the OECD's BEPS initiative;
- since 2017 (and including prior years as part of a transition), the spontaneous exchange of Tax Rulings, also in line with the Island's commitment to the OECD's BEPS initiative;
- matters related to the EU Code of Conduct for Business Taxation and EU Listing Process (from 2016), which includes the Island's commitment to address matters in relation to Tax Transparency, Fair Taxation and Compliance with anti-BEPS measures by 31 December 2018 – including new Substance legislation that has been approved by Tynwald and will result in companies filing new income tax returns from January 2020, that include information relating to the company's economic substance in the Island and subject to the appropriate legal basis being in place, will result in information being exchanged automatically with partner jurisdictions. Exchangeable information includes, for example, the identity of the beneficial owner(s) of the company.

Through these commitments, the Assessor shares tax data with approximately 100 countries. The same information is also being received by the Assessor in respect of Isle of Man taxpayers, and tax authorities across the world are already using this information to improve compliance with the domestic tax laws that are in place.

In 2017 the IoM retained the top "compliant" rating as part of the peer review rating undertaken by the OECD Global Forum on Transparency and Exchange of Information for Tax Purposes (the Global Forum).

Appendix 3 Terrorist Financing Sanctions and Proliferation Financing Sanctions

The Customs and Excise Division of the Treasury is responsible for financial sanctions and export and trade control measures, and has a good working relationship with the United Kingdom HM Treasury and Foreign and Commonwealth Office, (Export Control Joint Unit), as well as with HM Revenue and Customs, Border Force and the National Crime Agency.

UN sanctions in relation to TF and PF are implemented in the IoM through legislative means contained in the Terrorism and Other Crime (Financial Restrictions) Act 2014 and application of EU sanctions law. UN, EU and UK sanctions lists are monitored daily for updates and news releases published by CED. The regulators highlight the CED news feed in their Handbooks and on their websites.

Since 2015 there has been improved awareness of sanctions within law enforcement agencies and the regulators, with sanctions matters being discussed in the relevant AML/CFT meetings. Details of the TF and PF sanctions regime are now specifically included within the AML/CFT Code and Handbook for industry.

A 'Proliferation and Proliferation Financing Risk: Policy Protocol' was approved and formally adopted by the IoM Government and published in 2017. During 2018 the IoM also further developed and improved the guidance and outreach on sanctions, in particular to ensure that financial sanctions, sanctions relating to terrorist financing and sanctions relating to proliferation financing are clearly differentiated for industry. This was achieved by a substantial revision and updating of existing guidance, including making clear about the reporting obligations and when assets must be frozen; by a revision and updating of the sanctions website to make it more accessible for users, and by the production of an internal guidance manual on handling sanctions matters. The IOMFSA also updated the Anti-Money Laundering and Countering the Financing of Terrorism Handbook to include enhanced guidance on proliferation, TF and the IoM Sanctions Regime. The GSC also enhanced its published guidance in these areas. Businesses are making reports of suspected breaches of sanctions to the FIU (7 have been received since January 2019), but none have been in relation to TF or PF. Those reports have been investigated and it was found that no actual breaches of sanctions have been made[55].

Proliferation financing can also be linked to trade based money laundering (TBML). While many of the businesses in the regulated sector are aware of the need to screen accounts and transactions for sanctioned individuals or entities, and to report any suspected breaches to the FIU, there is a potential risk that non-regulated businesses could become involved in transactions without understanding the sanctions regimes. The Island does not have a large manufacturing industry, and not many of the goods would be subject to export controls; however those that are involved in such controlled goods are aware of their obligations, with good cooperation between CED and the Export Control Joint Unit in the UK. There is, as a result, a reduced risk that proliferation goods will be supplied by Island based manufacturing companies. The greater risk is that TCSPs will be used to operate companies involved in making these types of supplies between two third countries or the financial services connected to making them. The guidance published by CED provides information on what industry should look out for, including typologies.

[55] For example, suspected sanctions breaches are reported which are in fact US OFAC or US BIS Entity Listings, neither of which are applicable in IoM law as financial sanctions breaches.

In 2019 the UK's Office for Financial Sanctions Implementation set-up a virtual network of sanctions administrators which includes members from the UK, the Crown Dependencies and Overseas Territories of the UK. CED is a member of this group and has already shared guidance with members of the group.

Appendix 4 NRA Scope and Methodology

The IoM uses the World Bank's National Risk Assessment Tool to guide the risk assessment process; the Tool was first adopted by the IoM for the 2015 NRA.

The overall national picture has been informed by data from the FIU, law enforcement and the regulators as well as economic data. A full review of the strength of the national measures in place to combat ML and TF has also been undertaken. These show improvement, with evidence of the actions taken and the investment made since the 2015 NRA and subsequent MONEYVAL report.

At industry level a focus for the 2019 NRA has been a full re-assessment (and in the case of some sectors the first full assessment) of DNFBPs by the authorities. The 2019 NRA has also included new sections covering cash; beneficial ownership; and legal persons and legal arrangements.

The NRA was coordinated by the AML/CFT Policy Office working with the following authorities;

Economic Crime Unit, Isle of Man Constabulary	Financial Intelligence Unit
International Cooperation and Asset Recovery Team, Attorney General's Chambers	IOM Financial Services Authority
Customs and Excise Division, Treasury	Gambling Supervision Commission
Income Tax Division. Treasury	Companies Registry, Department for Enterprise
IOM Courts of Justice	IOM Post Office

The views and contributions of the following professional and industry bodies were also sought as part of the NRA process (see below). Where there was no formal representative body in place the AML/CFT Policy Office engaged with identified individuals from that sector. The draft NRA was also shared with the AML/CFT Industry Advisory Group for comment.

Association of Chartered Certified Accountants	Association of Corporate Service Providers
Chartered Institute of Securities and Investments	Christian Aid & One World Centre Trustees
CoinCorner	Financial Planners & Insurance Brokers Association
IoM Online Gambling AML Forum	Institute of Chartered Accountants of England and Wales
IoM Association of Pension Scheme Providers	IoM Bankers Association
IoM Captive Association	IoM Estate Agents and the Royal Institute of Chartered Surveyors
IoM Wealth & Fund Services Association	Manx Insurance Association

Glossary

AGC	Attorney General's Chambers
AML / CFT	Anti-Money Laundering / Combating Financing of Terrorism
AML / CFT Code 2019	Anti-Money Laundering and Countering the Financing of Terrorism Code 2019
ARU	Asset Recovery Unit
ATCA 2003	Anti-Terrorism and Crime Act 2003
CDD	Customer / Due Diligence as defined in the AML/CFT Codes
CED	Custom and Excise Division (of Treasury)
CTA	Common Travel Area
CVC	Convertible Virtual Currency
DBRO Act	Designated Businesses (Registration and Oversight) Act 2015
DfE	Department for Enterprise
DNFBP	Designated Non-Financial Business or Profession
DTA	Double Taxation Agreements
ECU	Economic Crime Unit (of the IoM Constabulary)
EDD	Enhanced Due Diligence
EoN	Exchange of Notes
FATCA	Foreign Account Tax Compliance Act (of the USA)
FATF	Financial Action Task Force
FCSB	Financial Crime Strategic Board
FIs	Financial Institutions
FIU	Financial Intelligence Unit
FSA08	Financial Services Act 2008
Gambling Code 2019	Anti-Money Laundering and Countering the Financing of Terrorism (Gambling) Code 2019
GSC	Gambling Supervision Commission
HNWI	High Net Worth Individual
HVGD	High Value Goods Dealer

ICART	International Cooperation and Asset Recovery Team
ICT	Information and Communications Technology
IFA	Independent Financial Advisor
ILOR	International Letters of Request
	Isle of Man
IOMC	Isle of Man Constabulary
IOMFSA	Financial Supervision Commission
ITD	Income Tax Division (of Treasury)
LEAs	Law Enforcement Agencies
MER	Mutual Evaluation Report
ML	Money Laundering
MLAR	Mutual Legal Assistance Request
MLRO	Money Laundering Reporting Officer
MONEYVAL	Council of Europe's committee of experts on money laundering and terrorist financing
MOU	Memorandum of Understanding
MTIC fraud	Missing Trader Intra-Community fraud
NPO	Non-Profit Organization
NRA	National Risk Assessment
OECD	Organisation for Economic Co-operation and Development
OFI	Other Financial Institution
OFT	Office of Fair Trading
PEP	Politically Exposed Person
PF	Proliferation Financing
POCA 2008	Proceeds of Crime Act 2008
RLP	Registered Legal Practitioner
SAR	Suspicious Activity Report
SNPO	Specified Non-Profit Organisation
TBML	Trade Based Money Laundering

TCSP	Trust and Corporate Service Provider
TF	Terrorist Financing
TFS	Terrorist Financing Sanctions
TIEA	Tax Information Exchange Agreement
TOCFRA 2014	Terrorism and Other Crime (Financial Restrictions) Act 2014
Tynwald	Parliament of the Isle of Man
UBO	Ultimate Beneficial Owner
Unregulated Trustees Code	Anti-Money Laundering and Countering the Financing of Terrorism (Unregulated Trustees) Code 2018