COMMITTEE OF EXPERTS ON THE EVALUATION
OF ANTI-MONEY LAUNDERING MEASURES AND
THE FINANCING OF TERRORISM (MONEYVAL)

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

MONEYVAL(2016)25

Anti-money laundering and counter-terrorist financing measures

Isle of Man

Fifth Round Mutual Evaluation Report

December 2016

The Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism - MONEYVAL is a permanent monitoring body of the Council of Europe entrusted with the task of assessing compliance with the principal international standards to counter money laundering and the financing of terrorism and the effectiveness of their implementation, as well as with the task of making recommendations to national authorities in respect of necessary improvements to their systems. Through a dynamic process of mutual evaluations, peer review and regular follow-up of its reports, MONEYVAL aims to improve the capacities of national authorities to fight money laundering and the financing of terrorism more effectively.

The fifth round mutual evaluation report on Isle of Man was adopted by the MONEYVAL Committee at its 52nd Plenary Session (Strasbourg, 8 December 2016).

CONTENTS

EXECUTIVE SUMMARY

1. This report provides a summary of the AML/CFT measures in place in the Isle of Man ("IoM") as at the date of the on-site visit (25 April - 7 May 2016). It analyses the level of compliance with the FATF 40 Recommendations and the level of effectiveness of the IoM's AML/CFT system, and provides recommendations on how the system could be strengthened.

Key Findings

- The coordination of anti-money laundering/countering the financing of terrorism ("AML/CFT") policies in the IoM is a strong point. The AML/CFT Strategic Group, assisted by the AML/CFT Technical Group, takes the lead in this area and has been extremely active in promoting sound AML/CFT policies and bringing about significant reforms. The Strategic Group was at the time of the on-site visit overseeing the implementation of an action plan based on the findings of the NRA. It is expected that the action plan, once completed, will result in significant improvements across many areas within the IoM's AML/CFT regime.
- As a result of the National Risk Assessment ("NRA") completed in 2015, the authorities have a thorough understanding of where the money laundering ("ML") and financing of terrorism ("FT") vulnerabilities lie within the national institutional and legal framework. They are also aware of which sectors are most vulnerable to ML/FT, both through years of experience in supervision and a reasonably comprehensive assessment, conducted as part of the NRA process, of the products, services and customers present in the IoM.
- While the authorities are aware that the ML/FT threats are mainly external, their understanding of threats may be incomplete due to (a) the limited aggregated data available on the volume and destination of outgoing and incoming flows of funds in the financial sector and (b) the absence of aggregated data on where the beneficial owners of assets managed or funds held in the IoM are from or which countries those funds are coming from. The absence of this data creates challenges in determining whether any flows leaving the IoM could potentially be linked to FT, terrorist groups or individual terrorists in other countries, especially in high-risk jurisdictions.
- Financial intelligence generated by the financial intelligence unit ("FIU") has been used successfully by the Financial Crime Unit of the IoM Constabulary ("FCU") to develop evidence and trace criminal proceeds in some significant ML cases. However, other than those few cases, the FIU conducted limited in-depth analysis and, as a result, the intelligence products of the FIU only occasionally added significant value. The intelligence chain appears to be hampered by the low quality of suspicious activity reports ("SARs") received from reporting entities and the absence of reports on suspicions identified at the borders from the Customs and Excise Division ("CED").
- The authorities have been successful in prosecuting and achieving convictions for all types of ML, including self-laundering, third party ML and stand-alone ML. However, the number of convictions achieved is modest and the results do not reflect the risk-profile of the IoM. In the period under review, there were no domestically-initiated ML cases involving foreign predicate offences. Very few parallel financial investigations have been conducted. The FCU does not appear to take a proactive approach to identify, initiate and prioritise ML cases focusing on more complex cases, involving potential abuse of or by the IoM financial sector where property is the proceeds of foreign predicates. This also has an effect on the confiscation of proceeds of crime, since they are not identified through financial investigations and restrained at a very early stage. The overall value of property restrained and confiscated remains extremely low.

- The authorities have not, to date, detected any potential cases of FT and therefore have not had the opportunity to demonstrate the effective investigation and prosecution of FT. This may be partly explained by the lack of awareness and proactive approach in relation to potential suspicions of FT. A number of cases were noted where potential FT activities should have been at least considered for investigation, especially in relation to FT SARs, matches with United Nations Security Council Resolutions ("UNSCRs") and one mutual legal assistance ("MLA") request. There is no local dedicated anti-terrorism unit although training has been provided to some police officers.
- The IoM provides constructive and timely MLA, especially with respect to requests for restraint orders. Informal cooperation is conducted effectively to a large extent. The authorities regularly seek assistance from the United Kingdom ("UK"), although much less frequently from other countries.
- Financial institutions ("FIs") and designated non-financial businesses and professions ("DNFBPs") assess ML/FT risk at business level, apply a risk-based approach to CDD and generally demonstrate knowledge of AML/CFT requirements. However, the evaluators are of the opinion that there is insufficient understanding of risks where FIs operate relationships for intermediary customers and where use is made of customer due diligence ("CDD") information presented by third parties that have collected this information in turn from other parties ("information chains"). It is not clear that this inherent risk is being mitigated. Overall, the number of customers assessed as presenting a higher risk appears low compared to risks inherent in the IoM. There is no comprehensive requirement to have an independent audit function (in relation to certain FIs and DNFPBs) to test the AML/CFT system.
- Compliance by FIs and DNFBPs with AML/CFT requirements is actively supervised by the Financial Services Authority ("IOMFSA") and the Gambling Supervision Commission ("GSC"). However, the current legislative framework for supervising compliance by DNFBPs (except trust and corporate service providers ("TCSPs") and online gambling operators, which have been subject to supervision for a number of years) is still very new as is the application of a risk-based approach by the GSC. Furthermore, the IOMFSA does not routinely collect statistics and information that allow it to fully consider ML/TF risk in the financial sector as a whole and at sector level. Nor has the risk that arises from the use made by banks of CDD information provided through chains of introductions received sufficient attention from the IOMFSA. There has been over reliance in the past by the IOMFSA on the use of remediation plans to address AML/CFT issues, though steps have been taken to address this issue.
- Measures to prevent the misuse of legal persons and legal arrangements for ML and TF are based around the IOMFSA's long-standing regulation and supervision of TCSPs (which, unlike in many other countries, is not limited to AML/CFT compliance). However, it is common for TCSPs not to meet their customer (or beneficial owner(s) thereof) and to use professional intermediaries to collect (and certify) CDD information; and so there is an increased inherent risk that they may be provided with incomplete or false information.
- Measures do not extend to all trusts governed by IoM law. The authorities have not considered cases where legal persons and trusts established under IoM law have been used to disguise ownership or to launder the proceeds of crime.

Risks and General Situation

2. The IoM is an international financial centre. The national income accounts for the year 2013/14 show that financial services (banking, insurance, other finance and business services, legal and accounting services, and corporate services) account for 37.8% of its gross domestic product

("GDP") of GBP 4.32 billion[1]. However, online gambling has now replaced insurance as the largest economic sector on the IoM, with a 16.7% share of GDP, and information and communication technology and online gambling were the main drivers of growth during the year, growing by 58% and 30% respectively in real terms.

3. The NRA acknowledges that since much of the financial business is conducted on a non-face-to-face basis via intermediaries, the potential for proceeds of crime/funds related to ML/FT flowing into or through the IoM is medium-high. The ML threat is mainly external. Business generated outside the IoM is considered by the authorities to present the greatest source of threat. This is due to the volumes generated by non-resident customers and the type of non-resident customers that are targeted by service providers, such as high net worth individuals, which could include politically exposed persons ("PEPs"). The NRA identifies that as the largest financial partner for the IoM, the UK is by far the most frequently reported jurisdiction in terms of SARs. Corruption, tax evasion and fraud are thought to be the most likely external threats to the IoM. Domestic ML threats are less significant. The authorities have conducted an assessment of FT risk and concluded that the risk is medium-low. This conclusion is based on an assessment of a comprehensive set of factors. However, the assessment of the FT threat appears to be missing an important element, i.e. an assessment of the flows leaving the IoM, which could potentially be linked to the financing of terrorism, terrorist groups or individual terrorists in other countries, especially in high-risk jurisdictions.

4. The sectors which are considered to be most vulnerable to ML/FT are the trust and corporate services, banking, insurance and online gambling. Most customers of TCSPs are non-resident and many have a high net worth. Structures established for customers can also be complex and can be established for trading purposes, which adds to both complexity and risk. Banks may place reliance on CDD measures applied by TCSPs and other professional intermediaries and business is often referred by introducers. The online gambling and life insurance sectors are considered to be vulnerable to ML/FT due to their size, rather than due to any inherent features of the business that increase vulnerability. Given that the IoM is a centre for the creation of legal persons and trusts for non-resident persons, the potential for abuse may be greater. However, the IoM has taken measures to mitigate this risk. For instance, TCSPs, which manage a large majority of legal persons and trusts set up in the IoM, are subject to full regulatory control and supervisory visits have been conducted since 2000 in respect of Corporate Service Providers and 2005 in the case of Trust Service Providers.

Overall Level of Effectiveness and Technical Compliance

5. Following the last IMF evaluation in 2009, the IoM has made some important reforms to its AML/CFT framework. In particular, it has removed a number of barriers to ML prosecutions, extended the scope of the IOMFSA's supervisory regime to cover all DNFBPs (including lawyers and accountants) and has provided its FIU with additional powers to analyse STRs. The IoM has a strong legal and institutional framework for combating ML and TF, and overall its technical compliance framework is strong. However, improvements are still needed in respect of the transparency and beneficial ownership of legal persons and legal arrangements, internal controls in online gambling operators, and sanctions that may be applied by the GSC.

6. In terms of effectiveness, the IoM achieves substantial results with respect to two of the Immediate Outcomes ("IO"), moderate results with respect to six IOs and low results with respect to three IOs.

Assessment of Risks, coordination and policy setting (Chapter 2 - IO.1; R.1, R.2, R.33)

7. The authorities conducted a NRA in 2015 to understand the risks that the IoM faces. Risks were considered from the point of view of cross-border and domestic threats, vulnerabilities in the

[1] www.gov.im/about-the-government/offices/cabinet-office/economic-affairs-division.

national system and vulnerabilities in the financial and non-financial sectors. The NRA accurately reflects and represents the authorities' understanding of risk.

8. As a result of the NRA, the authorities have a thorough understanding of where the vulnerabilities lie within the national institutional and legal framework. They are also aware of which sectors are most vulnerable to ML/FT, both through years of experience in supervising the sector and a reasonably comprehensive assessment, conducted as part of the NRA process, of the products, services and customers present in the IoM.

9. The cross-border ML threats are assessed by looking at various factors, such as SARs, MLA requests and sectorial data. The understanding may be incomplete due to the limited aggregated data available on the volume and destination of outgoing and incoming flows of funds in the financial sector and the absence of aggregated information on where the beneficial owners of assets managed or funds held in the IoM are from or which countries those funds are coming from. The NRA considers the FT threat from various angles, with well-considered conclusions. However, it does not assess the threat of the IoM being used as a conduit for financial flows intended to finance terrorism, terrorist groups or individual terrorists in other countries, especially in areas of conflict high-risk jurisdictions.

10. The authorities coordinate the development of AML/CFT policies and activities through the AML/CFT Strategic Group, which is assisted by the AML/CFT Technical Group. The Strategic Group was at the time of the on-site visit overseeing the implementation of the action plan based on the findings of the NRA. Operational cooperation between the competent authorities is in most cases effective. However, there are some areas where further improvements are needed, especially in relation to FT investigations, the implementation of targeted financial sanctions ("TFS") and the control of the borders for the identification of non-declared or falsely declared cash.

Financial Intelligence, Money Laundering and Confiscation (Chapter 3 - IOs 6-8; R.3, R.4, R.29-32)

11. Financial intelligence is generated by the FIU, which was situated within the FCU during most of the evaluation period. Both the FIU and the FCU have access to a wide range of administrative, law enforcement and financial information sources. The FIU regularly seeks and obtains information to conduct its analysis.

12. Intelligence generated by the FIU has assisted the FCU in some important ML cases which have resulted in the identification of a prevalent typology in the IoM and, in one particular case, the conviction of 19 persons for ML. However, overall, the FIU conducted limited in-depth analysis and, as a result, the intelligence products of the FIU only occasionally added significant value. The analysis process of the FIU generally consisted in linking incoming SARs with existing ones and seeking information from databases and other domestic and foreign authorities to determine the suspect's economic profile and establish a link to an underlying criminal activity.

13. The criminal justice system effectively detects, investigates and prosecutes criminality affecting domestic security such as fraud, theft and drug crimes, and the corresponding ML offences. Nevertheless, ML is not sufficiently detected and investigated with regard to suspicion arising from SARs, identified by supervision of financial institutions and DNFBPs, or by harvesting information from incoming MLA requests.

14. Parallel financial investigations are conducted but not systematically and not in cases where the associated predicate offences occur outside the IoM. This is considered to be a material shortcoming in the system in view of the IoM's context and risks.

15. The authorities have in the past prosecuted all types of ML cases, including self-laundering, third party laundering and stand-alone cases of ML. However, the investigation and prosecution of ML in recent years have not been in line with the risks faced by the IoM, and is over focused on

domestic crime predominantly drug or fraud cases with relatively low proceeds. In recent years, no third party or stand-alone ML cases have been pursued, for instance, when involving complex structures or when used to launder foreign predicate criminality.

16. When offenders are successfully prosecuted the courts apply sanctions, though these seem low and not dissuasive.

17. The IoM's legal framework on restraint and confiscation is comprehensive. However, the authorities do not pursue the confiscation of proceeds of crime as a policy objective. The legal principle of proportionality is over-relied on when applying for confiscation, which in some cases has led to a situation where not all possible assets have been confiscated.

18. The overall value of property restrained, confiscated, and actually recovered remains extremely low and does not reflect the risks in the IoM. The focus is mainly on the restraint and confiscation of proceeds from predicate crime. The robust civil recovery framework introduced in 2009 is not applied in practice by the IoM authorities in relation to property, other than cash. There are no mechanisms for managing complex structures or assets other than funds.

19. The confiscation of falsely or undeclared cross-border cash and bearer negotiable instruments (BNIs) that are suspected to relate to ML/TF and associated predicate offences is not applied as an effective, proportionate and dissuasive sanction.

Terrorist Financing and Financing Proliferation (Chapter 4 - IOs 9-11; R.5-8)

20. The IoM assessment of the threat of the IoM being used as a conduit for financial flows intended to finance terrorism, terrorist groups or individual terrorists in other countries, especially in high-risk jurisdictions lacks sufficient consideration. A number of issues limit the effective pursuit of FT cases, including limited exchange of information between the authorities involved in the prevention and detection of FT, insufficient training provided to the authorities with FT competences, the lack of FT-specific procedures and the absence of relevant guidance to FIs and DNFBPs.

21. As of April 2016, TFS are implemented without delay in compliance with UNSCR 1267 and its successor resolutions, as well as UNSCR 1373. The overall level of awareness seems to be satisfactory, though some sectors (such as TCSPs, securities, insurance and on-line gambling sectors) require additional guidance. There have been cases where assets were frozen under TFS.

22. A positive element in the system is that a large majority of FIs and DNFBPs make extensive use of screening to identify persons designated under UNSCRs. There seems, however, to be an undue focus by both FIs and DNFBPs (and their supervisors), as well other competent authorities, on applying screening software (such as World-Check, Dow Jones etc.) to their databases. FIs and DNFBPs do not take additional measures to ensure that funds or assets are not jointly owned or controlled, directly or indirectly, by designated persons or entities and third parties are subject to freezing; however this is only in relation to parties who do not meet the FATF definition of beneficial owner or other relevant parties who are not already identified as directors, trustees, signatories etc.). The private sector was not clear as to the steps to be taken should assets held by complex structures be detected in the future (e.g. appointing a receiver to hold the shares, court-appointed directors to manage the activities of the company, etc.).

23. In terms of supervision, the discussions with the industry revealed that the monitoring and the control activities are often limited to the implementation of TFS, based on the screening exercise. Moreover, there is insufficient guidance on how to apply FT and PF sanctions. The mechanism to notify reporting entities of new designations is not comprehensive.

24. A risk-based regime for the supervision of non-profit organisations ("NPOs") has been introduced. However, it has not yet been fully implemented. Further work is needed with regard to the risk posed by unregistered NPOs which are not considered charities. Further work is also needed

with regard to the monitoring of additional potential FT-risks, such as those arising from financial activity of foreign NPOs and from transfers of funds to high-risk jurisdictions.

25. The presence of complex financial structures, private sector participants' over-reliance on commercial databases in higher risk cases, as well as challenges in the effective identification of beneficial ownership within the banking system (in cases when relying on a chain of introducers or other high risk situations such as pooled accounts), have a negative impact on the effectiveness of TFS. So does the fact that some market participants look for designated persons and entities only in higher risk cases.

26. There are formal mechanisms in place for the co-ordination of policies and activities concerning the combating the financing of proliferation of weapons of mass destruction. Matters concerning financing of proliferation are discussed on an on-going basis within the AML/CFT Strategic Group, with a view to taking measures to ensure that the country is compliant with the international standards in this area.

Preventive Measures (Chapter 5 - IO4; R.9-23)

27. Whilst some exceptions were noted, FIs and DNFBPs generally demonstrated good knowledge of requirements of the AML/CFT Code.

28. FIs and DNFBPs apply a risk-based approach, and hence apply enhanced CDD for higher risk customers. However, the number of customers assessed by some FIs and DNFBPs as presenting a higher risk appears to the evaluators to be low, compared to the risks that are inherent in the IoM's business model. The evaluators are concerned that enhanced CDD, including enhanced monitoring, will not be applied in any cases where customers that actually present a higher ML/TF risk are not rated accordingly, although it is recognised that the AML/CFT framework in place for insurers requires all insurers to obtain source of wealth as standard reflecting the higher inherent risk presenting in this sector.

29. There is insufficient understanding of ML/TF risk where FIs operate business relationships for intermediary customers (FIs and DNFBPs) and do not hold information on underlying customers.

30. FIs (particularly banks) and DNFBPs may use CDD information presented by a third party (especially TCSPs that present the greatest inherent ML/TF risk to the IoM) that has itself collected this information from another party – an information chain. Because of this chain, there is an increased inherent risk that a FI or DNFBP may have been provided with incomplete or false information and so unable to understand the nature of the customer's business and its ownership and control structure. In particular, the NRA notes that TCSPs often do not meet their customer (or beneficial owner(s) thereof) and many accept business from professional intermediaries.

31. The quality of SARs is rather low, with less than one third based on suspicion of ML/FT or underlying criminality.

32. All FIs and DNFBPs regulated under the FSA 2008 and IA 2008 are required to have appropriate and independent internal audit and compliance procedures, though some securities firms have not set up such an audit function. There are no similar requirements in the AML/CFT Code or Online Gambling Code. Accordingly, such functions are not always found in online gambling operators. Where in place, e.g. life assurance companies, they do not always cover AML/CFT issues.

Supervision (Chapter 6 - IO3; R.26-28, R. 34-35)

33. Supervisory actions in all fields are effective in preventing criminals and their associates from being directors and beneficial owners of FIs, TCSPs, online gambling operators and casinos. At the time of the onsite visit, the registration of other DNFBPs was still on-going and so its effectiveness could not be fully assessed.

34. The IOMFSA does not routinely collect statistics and information that allow it to fully consider ML/TF risk in the financial sector as a whole and at sector level.

35. The AML/CFT supervisory framework appears quite robust, with a variety of off-site factors examined and comprehensive on-site examination/follow-up being conducted. However, the IOMFSA has not given sufficient attention to the interplay of risks it is faced with in the banking and TCSP sectors, where there are chains of introductions and where TCSPs often do not meet the customer (or beneficial owner(s) thereof) and use a professional intermediary to collect that information.

36. There is a wide range of sanctioning tools available to the IOMFSA. However, there are gaps in the supervisory and sanctioning powers available to the GSC.

37. Past supervisory action appears commensurate with the IOMFSA's perception of risks. Whilst remediation action taken by the IOMFSA has not always been effective, the supervisor has already taken steps to address this issue. The current concentration of enforcement action is significant, and warrants an increase in staffing in this part of the supervisor.

38. Whilst the GSC has supervised AML/CFT compliance since 2011, this has until recently been based on a rolling programme of visits. Only recently has the GSC completed the work necessary to implement a risk-based approach. This means that it is not possible to assess the effectiveness of its risk-based approach at this time. Supervision under the DBRO Act of FIs and DNFBPs not otherwise overseen by the IOMFSA or GSC started only at the beginning of 2016, though members of the Law Society of the IoM and some accountants have been proactively supervised for AML/CFT purpose since 2011. These gaps in supervision have an impact on effectiveness.

Transparency of Legal Persons and Arrangements (Chapter 7 - IO5; R. 24-25)

39. The extent to which legal persons and legal arrangements can generally be misused for ML/TF purposes is well understood. However, no exercise has been conducted to specifically consider how legal persons and legal arrangements established under IoM legislation, have been used to disguise ownership or to launder the proceeds of crime.

40. Whilst basic information is available online, the Central Registry does not collect all the basic information listed under c.24.3 for foundations or partnerships, or collect it on a timely basis for 2006 companies. Like in many other jurisdictions, the Registrar does not ensure that basic information provided to it by legal persons is accurate.

41. Extensive reliance is placed on TCSPs to hold beneficial ownership information. CSPs have been regulated and supervised in the IoM since 2000 and TSPs since 2005 and, unlike in many other jurisdictions, regulation is not limited to compliance only with AML/CFT legislation. This provides a strong basis upon which to prevent the misuse of legal persons and legal arrangements. However, it is common for TCSPs not to meet customer(s) (or beneficial owner(s) thereof) and use is made of professional intermediaries to collect beneficial ownership information. This has an impact on the effectiveness of measures to prevent misuse.

42. In the case of 1931 companies, which need not be administered by a TCSP, beneficial ownership information is held by a nominated officer. However, as a result of legislative gaps and the possibility that the beneficial owner of a company might be another legal person (explained under c.24.6 in the TC annex), information held by such an officer may not be adequate, accurate or current.

43. Appropriate measures to prevent the misuse of trusts do not apply to arrangements that are governed by IoM law where the trustee is not resident in the IoM or is so resident, but does not act by way of business.

International Cooperation (Chapter 8 - IO2; R. 36-40)

44. The IoM provides constructive and usually timely mutual legal assistance across a range of international co-operation requests. Nevertheless, additional resources and procedures should be allocated in the future to ensure both effective investigation and prosecution of ML and in particular restraint and confiscation of criminal proceeds, especially in the early stages of a criminal investigation.

45. Excellent cooperation exists between the IoM and the UK, especially with regard to tax and customs matters. The IoM proactively seeks legal assistance and other forms of international co-operation from the UK. However, it has not done so systematically with other jurisdictions to pursue domestic ML, associated predicate offences and TF cases which have transnational elements. Efforts in this area should be increased, since it is one of the few avenues available to the authorities, which could assist in initiating domestic ML related to foreign predicate offending. Mechanisms and procedures are only now being put in place to harvest and use information in incoming MLA requests.

46. Overall, in the context of an international financial centre, the low number of outgoing requests does not seem commensurate with the IoM risk profile and points to the lack of a proactive approach.

Priority Actions

47. The prioritised recommended actions for the IoM, based on these findings, are:

• The authorities should identify, and then take steps to collect and maintain statistics on outgoing and incoming flows of funds in the financial sector. The IoM should then conduct a reassessment of those areas which would have benefitted from these statistics, mainly cross-border ML and FT threats.

• The stand-alone FIU should be more proactive in generating intelligence, in accordance with the risk profile of the IoM.

• The IoM should undertake a more detailed assessment of the risk resulting from the use by banks of CDD information provided by TCSPs that have collected this information in turn from a professional intermediary.

• The authorities should consider re-assessing the risk posed by lawyers, the real estate sector and the quality of border controls.

• The authorities should establish and apply a criminal justice policy on ML investigations and prosecutions. This should set out the circumstances in which ML investigations need to be initiated reflecting the risk of ML in the IoM, especially with regard to the laundering of proceeds of foreign predicate offences.

• Law enforcement authorities should systematically harvest intelligence from all incoming international requests to aid in the detection of potential opportunities for the effective investigation of ML suspicion regarding IoM based financial institutions and intermediaries.

• Develop a strategy to pursue the effective restraint and confiscation of both instrumentalities and proceeds of crime (and their corresponding value) as a high-level criminal justice policy objective, especially with regard to predicate offences committed abroad.

• Develop procedures for systematic initiation of parallel financial investigations aimed at the detection of potential criminal assets subject to confiscation (including restraint of potential criminal proceeds when these are detected prior to the formal initiation of a criminal investigation, e.g. upon foreign request).

• Adopt an independent CFT-strategy from which a clear policy for tackling FT can be developed.

• Taking account of risk, authorities should further limit the circumstances in which CDD information and evidence of identity presented by a third party can be used, including where that third party has collected information from another party (an information chain).

• Authorities should require FIs to take account of risks presented by underlying customers when applying CDD exemptions to intermediary customers under paragraph 21 of the AML/CFT Code. Application of the exemption should also be prohibited where specific higher risk scenarios apply. Requirements to sample-test whether CDD and record-keeping requirements are appropriately applied to underlying third parties should be reviewed and alternative measures put in place, as necessary, to mitigate risk.

• In accordance with findings of the NRA, the IOMFSA should collect statistics and information that will allow it to better consider ML/TF risk in the financial sector as a whole and at sector level; this includes information on the extent to which firms utilise concessions, including the use of introducers. In turn this should be used to enhance the IOMFSA's supervision of sectors, most notably TCSPs and banks, where the use of introducers and intermediaries is identified as an inherent risk in the NRA.

• More staff should be available for the supervision of entities under the DBRO Act and enforcement in the IOMFSA.

• As identified in the NRA, additional supervisory and sanctioning powers should be given to the GSC.

• Authorities should also take measures to satisfy themselves that companies, shareholders and nominated officers comply with requirements set in the CBO Act 2012 in order to ensure that accurate and current beneficial ownership information is available.

• The authorities should develop both a strategy and written policies to seek foreign assistance proactively through all available channels, upon suspicion of ML/TF or in relation to TFS.

Effectiveness & Technical Compliance Ratings

Effectiveness Ratings

IO.1	**IO.2**	**IO.3**	**IO.4**	**IO.5**	**IO.6**	**IO.7**	**IO.8**	**IO.9**	**IO.10**	**IO.11**
Sub.	Sub.	Mod.	Mod.	Mod.	Low	Low	Low	Mod.	Mod.	Mod.

Technical Compliance Ratings

R.1	**R.2**	**R.3**	**R.4**	**R.5**	**R.6**	**R.7**	**R.8**	**R.9**	**R.10**
LC	C	C	LC	LC	LC	LC	LC	C	LC

R.11	**R.12**	**R.13**	**R.14**	**R.15**	**R.16**	**R.17**	**R.18**	**R.19**	**R.20**
LC	LC	C	LC	C	PC	LC	LC	C	C

R.21	**R.22**	**R.23**	**R.24**	**R.25**	**R.26**	**R.27**	**R.28**	**R.29**	**R.30**
LC	LC	PC	PC	PC	LC	LC	LC	LC	C

R.31	**R.32**	**R.33**	**R.34**	**R.35**	**R.36**	**R.37**	**R.38**	**R.39**	**R.40**
C	LC	LC	LC	PC	LC	LC	LC	C	LC

MUTUAL EVALUATION REPORT

Preface

48. This report summarises the AML/CFT measures in place in the IoM as at the date of the on-site visit. It analyses the level of compliance with the FATF 40 Recommendations and the level of effectiveness of the IoM's AML/CFT system, and recommends how the system could be strengthened.

49. This evaluation was based on the 2012 FATF Recommendations, and was prepared using the 2013 Methodology. The evaluation was based on information provided by the IoM, and information obtained by the evaluation team during its on-site visit to the IoM from 25 April -7 May 2016.

50. The evaluation was conducted by an assessment team consisting of:

Evaluators

- Mr Yehuda Shaffer, Deputy State Attorney, Ministry of Justice, Israel (legal evaluator)
- Ms Stela Buiuc, Deputy Director, Center for Legal Approximation, Ministry of Justice. Republic of Moldova (legal evaluator)
- Mr Amar Salihodzic, International Affairs Officer, Financial Intelligence Unit, Liechtenstein (law enforcement evaluator)
- Mr Radoslaw Obczynski, expert in the AML/CFT Unit of the Polish Financial Supervisory Authority, Poland (financial evaluator)
- Mr Matis Mäeker, Lawyer, Finance Inspector, Business Conduct Supervision Division, Financial Supervisory Authority, Estonia (financial evaluator)

MONEYVAL Secretariat

- Mr Michael Stellini, Head of AML/CFT Monitoring and Training Unit
- Mr Andrey Frolov, Administrator
- Mr Andrew Le Brun, Administrator
- Ms Veronika Mets, Administrator

51. The report was reviewed by the FATF Secretariat, Mr Philipp Roeser (Liechtenstein) and Mr Borja Aguado (Andorra).

52. The IoM previously underwent an IMF Mutual Evaluation in 2009, conducted according to the 2004 FATF Methodology. The 2009 evaluation and 2013 follow-up report have been published and are available at http://www.coe.int/t/dghl/monitoring/moneyval/Countries/Isle_of_Man_en.asp.

53. The IoM's 2009 Mutual Evaluation concluded that the country was compliant with 12 Recommendations; largely compliant with 24; and partially compliant with 13. The IoM was rated compliant or largely compliant with 8 of the 16 Core and Key Recommendations.

CHAPTER 1. ML/TF RISKS AND CONTEXT

54. Located in the middle of the Irish Sea, the IoM is 33 miles long and 13 miles wide at its broadest point and has a total land area of 227 square miles. The resident population is 84, 497. In 2013/14, the IoM's GDP was GBP 4.32bn. The local currency is the Manx pound, which is in parity with the British pound (sterling).

55. The IoM's ancient parliament, Tynwald, is the oldest legislature in the world in continuous existence. Tynwald has two branches: the House of Keys and the Legislative Council.

Constitutionally, the IoM is a self-governing British Crown Dependency and, as is the case in the UK, does not have a codified constitution. The UK Government, on behalf of the British Crown, is ultimately responsible for the IoM's international relations. As the Head of State, the Queen is represented in the IoM by the Lieutenant-Governor.

56. The IoM has no party political system and the leader of its government, the Chief Minister, is chosen by Tynwald after each general election. The Chief Minister selects eight Ministers to head the major government departments and together they make up the Council of Ministers, the central executive body or IoM "Cabinet", which is accountable to Tynwald.

57. The IoM has its own legal system and jurisprudence, which is based on the principles of common law shared by many Commonwealth countries. Manx law does not automatically follow, and is not identical, to English law. There are separate Acts of Tynwald. Manx customary and common law has developed taking into account local conditions, the needs of the IoM and the developments in other common law jurisdictions. The IoM's High Court judges hold the ancient office of Deemster and have jurisdiction over all criminal and civil matters. There is a final right of appeal, with leave, against decisions of the Appeal Division to the Judicial Committee of the Privy Council.

ML/TF Risks and Scoping of Higher-Risk Issues

Overview of ML/TF Risks

58. The IoM is an international financial centre and, as such, it faces various ML/FT risks. The NRA published by the IoM in June 2015 acknowledges that since much of the financial business is conducted on a non-face-to-face basis via intermediaries, the potential for proceeds of crime/funds related to ML/FT flowing into or through the IoM is medium to high.

(a) ML threats

59. The NRA rates the ML threat, which is mainly external, as medium-high. The NRA considers the external ML threat from different angles by looking at data based on sectorial information (including assets and liabilities), SARs and incoming MLA requests. On the basis of this information, it is considered that business generated outside the IoM presents the greatest source of threat. This is due to the volumes generated by non-resident customers and the type of non-resident customers that are targeted by service providers, such as high net worth individuals, which could include politically exposed persons ("PEPs"). The NRA identifies that, as the largest financial partner for the IoM, the UK is by far the most frequently reported jurisdiction in terms of SARs. The NRA working group has suggested that, based on their experience, tax evasion, corruption and fraud are the most likely external threats to the IoM. This is corroborated by statistics on the number of incoming MLA requests[2]. The NRA also refers to a Transparency International report (2015 Publication) which implies that Manx companies hold real estate in London acquired through proceeds of corruption and bribery[3]. There have been very few investigations into the role of IoM based individuals and companies in cases of cross-border ML. However, financial flows into and out of the IoM represent a potential for illicit money to enter and to flow through the IoM.

60. Domestic ML threats are less significant. The NRA identifies local drug dealing and theft as the main proceeds-generating offences. However, estimates for the volume of undetected ML occurring domestically and the value of the proceeds of crime in circulation in the IoM do not exist. There have been a few cases detected where persons resident in the IoM were found to be involved in ML internationally.

(b) FT threats

[2] See Table 16 under IO2.
[3] These cases were investigated and only one case is still ongoing.

61. The NRA assesses the FT threat as medium to low. According to the NRA, there is little evidence of the IoM having been at risk of FT in recent years. This conclusion is based on, inter alia, the fact that few SARs relating to FT were submitted to the FCU; the geographical position of the IoM; the lack of domestic terrorism; the fact that there is no historical connection between the IoM and areas of conflict; the lack of residents who originated or have connections to areas of conflict or terrorist activity; low levels of FT MLA requests (one in 2011); and the fact that the IoM has never featured in international FT typologies. The authorities are supported in this view by the fact that the security services in the UK, with which the IoM work very closely on security issues, consider that the IoM is at low risk of terrorism and FT.

62. While these conclusions are not disputed, as an international financial centre, the IoM faces an enhanced threat of being used as a conduit for financial flows intended to finance terrorism, terrorist groups or individual terrorists in other countries, especially in high-risk jurisdictions. No such cases have been identified to date by the authorities. However, the possibility that this might have happened cannot be entirely ruled out since the authorities have not analysed the destination of flow of funds leaving the IoM. It appears that, notwithstanding the constitutional framework of the IoM, the authorities have not been sufficiently proactive domestically in identifying FT threats but have utilised information held by security services in the UK. The possibility that funds managed by foreign NPOs may have flowed through the IoM to support terrorist organisations in third countries has not been considered. This notwithstanding, the evaluation team agrees that, in terms of threats, FT is less material than ML, in the context of the IoM.

(c) ML/FT vulnerabilities

63. The TSCP sector is considered by the authorities to be the most vulnerable to ML/FT. The NRA rates the risk of TCSPs as medium-high. Most customers are non-resident and many have a high net worth. Customers also include online gambling operators, owners of aircraft and ships registered in the IoM, "exempt schemes" and money lenders, although these categories would constitute a small percentage of the entire customer base. Structures established for customers can also be complex and can be established for trading purposes, which adds to both complexity and risk (such as trade-based ML – identified as a risk in the NRA). Reliance may be placed by TCSPs on CDD measures applied by third parties and business is often referred by introducers. Like in other jurisdictions, there is an inherent risk of the TCSP sector being misused to facilitate ML, in particular, laundering the proceeds of foreign tax evasion, foreign corruption and organised crime, and FT through NPOs administered in the IoM.

64. The banking sector in the IoM is significant not only due to its size but also because of its relationship with other parts of the economy. For example, banks provide products and services to TCSPs, companies and trusts that are administered by TCSPs, online gambling operators, and lawyers. Banks may apply exemptions to customers in some cases, e.g. to pooled accounts operated by regulated persons providing wealth management.

65. Business in the insurance and pensions sector is predominately sourced from the UK (British expatriates) and products are distributed through independent financial advisors ("IFAs") who will often have face-to-face contact with their customers. IFAs can be small, independent operators, where sales (which trigger commissions) may receive more focus than preventative measures. The pensions sector is said to offer niche tax efficient solutions for non-resident entrepreneurs wishing to establish personal retirement benefit schemes.

66. With respect to the securities sector, the NRA identifies a number of areas where ML/TF risk could be elevated. In particular, risks are inherent in "exempt schemes" – unregulated private arrangements which have a capped number of investors. Funds with a limited number of investors are likely to present a higher risk. Risks are generally greater where the promoter and controllers (e.g. directors) of such funds are not resident in the IoM (which is quite common). The IoM has seen significant growth in non-retail overseas funds which also carries additional risks.

67. The IoM is one of the leading jurisdictions in terms of recognising the use of convertible virtual currencies (a term that includes crypto-currencies) and their regulation. Eleven firms have been registered under the DBRO Act and are subject to AML/CFT requirements. The authorities are monitoring this emerging new sector to establish what risks may arise from it.

68. The NRA identifies online gambling as posing a medium risk of ML/FT, noting that there is a medium level of threat and a medium level of vulnerability. According to the NRA, the vulnerability assessment reflects that the business is international and non-face to face but the risk factors are countered by a number of factors, such as the fact that the industry is almost exclusively IT based and transaction records are kept to an almost forensic standard. The threat is assessed as medium as no evidence was found that the sector was used for ML/FT purposes and very limited typologies are available generally. The risk is also somewhat mitigated since small sums are generally deposited by customers and operators have a vested interest in examining requests for the withdrawal of money.

69. Legal persons and legal arrangements in the IoM set up for non-residents may be vulnerable to ML/FT. The authorities have provided the evaluators with a case study on evasion of value-added tax that included an IoM company, which referred to the extensive use of IoM companies to hold real estate in London, and highlighted the use of Manx corporate structures in investigations started after the Arab Spring. The NRA highlights that companies incorporated under the Companies Act 1931 are not required to retain the services of a TCSP. Instead, they must identify a person who is responsible for holding details of beneficial ownership under the Companies (Beneficial Ownership) Act 2012.

Country's risk assessment & Scoping of Higher Risk Issues

(a) Country's risk assessment

70. The NRA, which was concluded in June 2015, uses the National Money Laundering and Terrorist Financing Risk Assessment Tool provided by the World Bank. The process was managed by the NRA Working Group, which comprises all domestic AML/CFT stakeholders. The Working Group was established by the IoM's Government's AML/CFT Strategic Group. The whole process was conducted with the assistance of World Bank experts. The NRA project manager was appointed from within the Cabinet Office. Seven sub-groups were established, including a group to examine national threats and one to examine national vulnerabilities[4]. The modules at national level (threats and vulnerabilities) were led by the relevant competent authorities, whereas the sector-specific modules were conducted with the involvement of the private sector, predominantly through their professional bodies. Higher risk areas and institutional gaps were identified as a result of the process and an action plan was drawn up by the authorities at the end of 2015 to address those risks and gaps.

71. The areas identified in the NRA as presenting the highest exposure to ML/TF risks are: (a) the international nature of business which has further implications with regard to domestic AML/CFT requirements, as well as the IoM`s approach to domestic and international cooperation; (b) deficiencies in financial intelligence and financial crime investigation; (c) deficiencies with regard to border controls.

72. With regard to the financial and non-financial sector, the NRA identified the following sectors as being the most vulnerable to ML/TF: (a) TCSPs (medium high); (b) insurance (medium); (c) online gambling (medium); (d) banking (medium).

73. The conclusions in the NRA appear reasonable. The NRA confirmed the authorities' views on certain vulnerabilities (e.g. those within the life insurance, banking, TCSPs and online gambling sector), while also bringing to the fore threats and vulnerabilities which had not previously been

[4] The seven sub-groups were the following: national threat assessment; national vulnerability assessment, banking sector vulnerability; securities sector vulnerability; insurance sector vulnerability; other financial institutions; and DNFBP sector vulnerability.

identified (e.g. gaps in the institutional framework and vulnerabilities posed by, for instance, payroll service companies).

74. The cross-border risks could not be considered to a sufficient degree since aggregate information on the volume, destination of outgoing and origin of incoming funds in the financial sector is not collected at national level. The authorities pointed out that the systematic collection of data, such as the balance of payments, is very difficult due to the absence of a central bank. They indicated, however, that the IoM participates in the reporting of statistics to the Bank for International Settlements ("BIS") and has data on banking activity directly into and from the IoM for over 250 countries which was considered as part of the threat assessment. Insurance and pensions, the largest FI sector in the IoM, considered data on the client base of regulated entities, which is analysed in the NRA against the level of FATF compliance of the relevant jurisdiction and ML risk. Data was also available on the domicile of collective investment schemes. The threat assessment identified that overall the largest exposure for the IoM came from the UK as the largest financial partner for the IoM and with strong economic and geographic links. Significant amounts of banking, insurance, securities and DNFBP business is directly connected to the UK. Careful consideration was given to the customer segments, products and services rather than any assumption that business with and via the UK represented low risk. Other jurisdictions were identified in the NRA using the same methodology. In addition, banks were requested to provide information covering one quarter's payment volumes (in/out, domestic and international, by specific currencies). At the time of the on-site visit, the authorities had already started a data collection process to rectify this shortcoming.

75. The NRA looks at the vulnerabilities of each sub-sector within the financial and DNFBP sector. The World Bank model requires that the financial sectors and DNFBPs undertake an assessment which includes products, services, client base profiles etc., as well as an assessment of general factors which can create vulnerability (or conversely help to combat misuses) of products/services and the sector as a whole. The process appears to have been conducted very diligently. The NRA contains sound conclusions on the sectors which are considered to represent a higher risk within the specific context of the IoM. However, the final NRA report does not indicate the specific products, services, geographical links and delivery channels that are present in the IoM which are higher risk. It should be noted however that the supervisors demonstrated that they have sufficient understanding of the specific vulnerabilities within the different sub-sectors. A similar understanding was not demonstrated by other authorities.

76. The NRA considers various factors to determine the level of FT threats. These are laid out in paragraph 61. It is the view of the evaluation team that the absence of reliable statistics on financial inflows and outflows through the IoM `s economy did not enable the authorities to fully assess TF threats, as it is not known where funds are actually transferred to, i.e. high-risk jurisdictions, jurisdictions and areas bordering with such and jurisdictions cooperating with high-risk jurisdictions. The extent to which funds managed by foreign NPO funds may have flowed through the IoM to fund terrorist organisations in third countries, was not considered in depth.

77. The NRA does not set out the prevalent typologies and methods which have been or may be used to launder funds/finance terrorism through the financial and non-financial sectors. It therefore fails to clearly identify the extent to which proceeds of crime are laundered in the IoM. At the time of the on-site visit, work had already been underway to ensure that the 2nd iteration of the NRA provides a more detailed view of risks.

(b) Scoping of higher risk issues

78. The assessment team identified those areas which required an increased focus through an analysis of information provided by the IoM authorities, including the NRA, and by consulting various open sources.

(i) Legal, operational and institutional issues

79. **Parallel financial investigations and financial intelligence analysis.** As identified in the NRA, the capacity and resources available for financial crime investigations and financial intelligence gathering and processing in the FCU are two critical areas with deficiencies. The NRA reveals that the FCU lacks experienced staff and appropriate AML/CFT training and there are concerns about the effectiveness of the basic functions of the FCU. Limited use of financial intelligence and incoming international requests appears to be made by law enforcement to develop evidence and trace criminal proceeds related to ML, associated predicate offences and TF. These areas received considerable attention on-site.

80. **Foreign predicate offences.** Notwithstanding its status as an international finance centre (IFC), in the period under review, there were no prosecutions for ML in the IoM on the basis of a foreign predicate offence and there were few investigations into the role of IoM-based individuals, companies and trusts in cases of cross-border ML. As a consequence, no convictions and confiscations have been achieved in this area. The evaluation team sought to determine the underlying causes hindering the process.

81. **International cooperation.** The evaluation team paid particular attention to the manner in which international cooperation is conducted by the Manx authorities, given the international nature of the business in the IoM. The authorities do not appear to proactively seek cooperation from their foreign counterparts, other than those in the UK, where suspicions have been reported by the private sector or are otherwise identified. Discussions were held on-site to determine the underlying reasons.

82. **Supervision of lawyers and accountants.** The IoM Law Society was responsible for self-regulating compliance of its members with AML/CFT requirements. As of March 2015, there were 226 practicing advocates employed across 36 practices (112 of which are employed by 6 practices). Similarly, accountants that are members of UK professional bodies were overseen by those professional bodies. Based in the UK, oversight may arguably be in line with UK assessments of risk rather than that of the Isle of Man. From October 2015, the Designated Businesses (Registration & Oversight) Act 2015 transferred the responsibility for AML/CFT oversight to the IOMFSA. The IOMFSA has delegated its oversight powers to certain professional bodies including the IoM Law Society, the Institute of Chartered Accountants in England and Wales (ICAEW), the ACCA and the IFA. The bodies act as agents of the IOMFSA, accordingly, the IOMFSA's coordination role is an important one. Onsite, consideration was given to the capacity for self-regulation of the legal profession in such a small jurisdiction and merits in delegating oversight of accountants to a body outside the jurisdiction.

(ii) Areas of increased focus in the financial sector

83. **The banking sector**. The effectiveness of customer due diligence ("CDD") measures applied by third parties is particularly important for the IoM, where a significant part of financial activities is conducted on a non-face-to-face basis and where it is understood that third parties represent a source of new business. Third parties may be "relied upon" to perform elements of the CDD process, or to introduce business. Particular attention was paid to how banks ensure that documents, data or information collected from such third parties are reliable and independent.

84. **The insurance sector.** The evaluation team sought to understand how insurance and pension companies ensure that documents, data or information collected from independent financial advisors are reliable and independent, particularly because it is not uncommon to find customers using trusts as asset-holding vehicles or as part of more complex structures.

85. **The "FinTech" industry.** The ML/TF implications in respect of the IoM's development as a centre for convertible virtual currencies were considered on-site. The IoM is one of the leading jurisdictions in terms of recognising the use of convertible virtual currencies (a term that includes crypto-currencies) and their regulation. The evaluation team considered the risk assessment conducted by the IoM authorities before promoting development opportunities in this area.

(iii) Areas of increased focus in the non-financial sector

86. **TCSP sector**. The evaluation team dedicated considerable time to meetings with this sector. The focus was on how well ML/TF risks are mitigated by TCSPs, in particular the identification of beneficial owners of TCSP clients.

87. **The Online gambling sector.** The evaluation team considered how well ML/TF risks are mitigated in this sector.

Materiality

88. The IoM is an international financial centre. In 2010, the Financial Stability Board ("FSB") included the IoM in its initiative to encourage the adherence of all jurisdictions to regulatory and supervisory standards on international co-operation and information exchange. The initial focus of this initiative was on the adherence of FSB members and "other jurisdictions that rank highly in financial importance". The IoM is also included in the Global Financial Centres Index which ranks the competitiveness of financial centres and is widely quoted as a source for ranking such centres. At March 2016, the IoM was placed in 68th place (out of 86 centres).

89. The IoM's national income accounts for the year 2013/14 show that financial services (banking, insurance, other finance and business services, legal and accounting services, and corporate services) account for 37.8% of its gross domestic product of GBP 4.32 billion[5]. However, online gambling has now replaced insurance as the largest economic sector on the IoM, with a 16.7% share of GDP, and information and communication technology and e-Gaming were the main drivers of growth during the year, growing by 58% and 30% respectively in real terms. The economy is diverse with around 25 active sectors.

90. The IoM's banking, insurance and pensions, and securities sectors held GBP 141.9 billion in assets at December 2014. The IMF's 2009 Financial Sector Assessment Program found financial sector regulation and supervision to be generally of a high standard, and supervisory efforts concentrated in those areas most relevant to the activities of FIs.

91. The importance of financial services to the economy is also reflected in employment statistics, with insurance, banking, finance and business services together employing slightly over 20% of the IoM's workforce (43,134 in 2011).

92. National income accounts show that 2013/14 was the thirtieth successive year of growth for the IoM's economy which expanded by 6.1%, or 4.5% in real terms (compared to 3.2% in 2012/13). Unemployment is low at 1.7%[6].

Structural Elements

93. The key structural elements for effective AML/CFT controls are present in the IoM. The IoM is generally considered to be a very stable democracy. Political and institutional stability, accountability, the rule of law and an independent judiciary are all well established. The IoM has made a clear high-level commitment to implement the FATF Standards, with a view to establishing an overall effective AML/CFT framework. Important reforms, triggered by the NRA process, have been recently set in train to address significant weaknesses in the system.

Background and other Contextual Factors

Overview of AML/CFT strategy

[5] www.gov.im/about-the-government/offices/cabinet-office/economic-affairs-division.
[6] www.gov.im/media/1351534/2016-05-17-q1-2016-economic-quarterly-report.pdf

94. The IoM Government published a formal commitment in 2012 to adopting the revised Financial Action Task Force (FATF) 40 Recommendations concerning International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation. Furthermore, the Council of Ministers has endorsed the *Isle of Man Government Anti-Money Laundering and Combating the Financing of Terrorism National Strategy 2016-2018 (The National Strategy)*[7] based on *Isle of Man Risk Assessment of Money Laundering and Financing of Terrorism(NRA).*[8]

95. The National Strategy identifies areas where the IoM Government will revise or enhance existing activities, review where new policies or guidance may be appropriate, and work with regulators and law enforcement to improve transparency. The National Strategy identifies three overarching strategic themes which underpin each of the 10 goals that make up the strategy. These themes are:

1) Monitoring and maintaining compliance with international obligations and standards and supporting measures aimed at tackling money laundering, terrorist financing and combating proliferation;
2) Ensuring that the Isle of Man Government's national risk assessment and risk appetite for anti-money laundering and combating the financing of terrorism is adopted nationally by government, regulators and industry;
3) Raising awareness and increasing knowledge concerning the threat of terrorist financing.

96. The 22 actions which were identified during the NRA process are included within the 10 goals which make up this National Strategy. The goals concern; international cooperation; policy and legislation; collection and analysis of data; the FIU; financial crime investigation; asset forfeiture and recovery; regulatory sanctions; DNFBP oversight; controls on cash and similar instruments at the border; and training and awareness of AML/CFT within Government,

97. Within each goal a lead agency has been identified with responsibility for reporting upon and delivering the required actions, or working with others where the actions are shared between agencies.

Overview of the legal & institutional framework

98. As regards ministries and operational agencies, the institutional framework in the IoM described in the 2009 MER (page 33-36) remains essentially unchanged, including their roles and responsibilities:

Policy and coordination

99. **The Council of Ministers**[9] is the highest level decision-making body within the IoM. It consists of small number of advisers, eight Ministers and the Chief Minister. Its purpose is to set national and international policy which includes matters in respect of AML/CFT and to provide clear leadership to the separate legal entities of departments, offices and statutory boards which make up the IoM Government. It also has some statutory decision-making functions and importantly has a reserved power to give a department or statutory board directions with regard to the exercise of functions where it appears to it to affect the public interest.

[7] Isle of Man Government Anti-Money Laundering and Combating the Financing of Terrorism National Strategy 2016-2018,https://www.gov.im/media/1350894/isle-of-man-government-aml-cft-national-strategy-2016-18.pdf

[8] Isle of Man Risk Assessment of Money Laundering and Financing of Terrorism, https://www.gov.im/media/1350893/isle-of-man-national-risk-assessment-2015.pdf

[9] National Strategy Appendix 1, https://www.gov.im/media/1350894/isle-of-man-government-aml-cft-national-strategy-2016-18.pdf

100. **The National Strategy Group ("NSG")**[10] is a committee of the Council of Ministers which is chaired by the Chief Minister. It is responsible for ensuring that priority is given to national imperatives within the National Strategic Plan, including AML/CFT matters.

101. **The AML/CFT Strategic Group** is a high-level committee consisting of senior officers from Government, the regulators and law enforcement, chaired by the Chief Secretary. The Strategic Group coordinates the development and implementation of cross government policies and activities for AML/CFT, proliferation and compliance with international standards and makes recommendations to the Council of Ministers on policy matters.

102. **The AML/CFT Technical Group**[11] provides advice and support to the AML/CFT Strategic Group in respect of the development of ML/FT regulation. It also advises on implications for the IoM of changes to international standards and the effectiveness of measures intended to tackle ML/TF at Government and industry level. The Technical Group comprises representatives from the regulators, law enforcement, the Treasury, the Cabinet Office and the Departments of Home Affairs and Economic Development.

103. **The Industry Advisory Group**[12] is a sub-group of the AML/CFT Strategic Group with its own terms of reference and is an industry liaison forum which brings together Government, regulators and industry. The work of this group feeds into the considerations of both the Strategic and the Technical AML/CFT groups.

104. **Ad hoc sub groups**[13] to the AML/CFT Technical Group and the Industry Advisory Group may be formed to consider particular issues.

105. **FIU Board**[14] is chaired by HM Acting Attorney General and brings together the Chief Constable and the Collector, Customs and Excise Division. The Board is attended by the Director, FIU. The Board members are also all members of the AML/CFT Strategic Group.

106. **The Cabinet Office**[15] plays a central role in the work of the Isle of Man Government, co-ordinating its corporate initiatives and managing its international relationships, including in the AML/CFT area. It is responsible for assessing risks and applying a risk-based approach, national cooperation and coordination, international instruments and international conventions.

107. **The Treasury Customs and Excise Division ("CED")**[16] is responsible for implementation of targeted financial sanctions related to terrorism and terrorist financing and targeted financial sanctions related to proliferation. The CED also has important law enforcement functions to perform and these duties can range from the investigation of local customs offences through to assisting other jurisdictions with the investigation of international money laundering. In the area of financial crime, the Division works closely with the Financial Crime Unit and contributes to the Chief Minister's Drug and Alcohol Strategy.

108. **The Treasury Income Tax Division ("ITD")**[17] responsibilities include all international matters affecting direct taxation and dealing with exchange of information requests at both a domestic and international level.

---

[10] Ibid.
[11] Ibid.
[12] Ibid.
[13] Ibid.
[14] Ibid.
[15] The Cabinet Office, https://www.gov.im/about-the-government/offices/cabinet-office/
[16] The Treasury Customs and Excise Division, https://www.gov.im/about-the-government/offices/cabinet-office/
[17] The Treasury Income Tax Division, https://www.gov.im/about-the-government/departments/treasury/income-tax-division/

109. **Department of Economic Development (the Central Registry)**[18] maintains the register and records of all companies and other business types incorporated in the Isle of Man, and provides a facility for the public to view documents which have been filed.

110. **Department of Home Affairs ("DHA")**[19] key aspect of its work is on anti-money laundering legislation and the associated documentation (higher risk countries).

Prevention and Detection

111. **The Isle of Man Financial Services Authority's ("IOMFSA")**[20] responsibilities include regulation and supervision of persons undertaking regulated activities in respect of deposit taking, insurance business, investment business, services to collective investment schemes, pensions, fiduciary services, spread betting and money transmission services, in or from the IoM and to conduct investigations into any potential liability arising from breach of AML/CFT legislation by persons undertaking regulated activities. The IOMFSA is now also the AML/CFT supervisor for all other financial institutions and DNFBPs (except casinos and online gambling), though in practice it is able (and does) delegate some aspects of supervision to the Law Society and UK accountancy bodies, although it retains all sanctioning responsibilities. IOMFSA supervises for AML/CFT purposes also captive insurance companies, and institutions like payroll agents and virtual currency operators going beyond the FATF standards (see IO3).

112. **Gambling Supervision Commission ("GSC")**[21] regulates all online gambling activities in addition to the licensing and regulation of land based gambling operations (casino, amusement and slot machines, known in the IoM as controlled machines, betting offices and lotteries).

Investigation and Disruption

113. **HM Attorney General's Chambers ("AGC")**[22] deal with civil and criminal matters for the Government of the Isle of Man. It also provides legal advice to Government Departments and Statutory Boards. The AGC also handles international letters of request.

114. **Financial Crime Unit ("FCU")**[23] is the investigative branch of the IoM Constabulary which is responsible for the investigation of ML and FT. It comprises 23 dedicated staff. Up until April 2016 the FCU was a joint police and customs department. It remains a Division of the IoM Constabulary.

Operational agencies

115. **Financial Intelligence Unit ("FIU")** is a joint police/customs unit supported by civilian personnel performing administrative functions. The independent FIU is constituted to serve as the national centre for receipt, analysis and dissemination of all relevant ML and TF information. Previously, the FIU of the IoM was established as a subsection of the FCU within the Constabulary, which acted as the first reception point of the disclosures and conducted an initial analysis of the information received. As a result of legislative changes in April 2016 in the form of the FIU Act 2016, the FIU was established in law as a standalone body corporate, independent of both the Constabulary and the CED, under the oversight of AGC and guidance from the FIU Board. The financial crime investigation function remained within the responsibility of the Constabulary.

Overview of the financial sector and DNFBPs

[18]Department of Economic Development Central' Registry, https://www.gov.im/about-the-government/departments/economic-development/central-registry/

[19] Department of Home Affairs, https://www.gov.im/about-the-government/departments/home-affairs/

[20] Isle of Man Financial Services Authority ("IOMFSA"), http://www.iomfsa.im/

[21]Gambling Supervision Commission, https://www.gov.im/about-the-government/statutory-boards/gambling-supervision-commission/

[22]HM Attorney General's Chambers ("AGC"), https://www.gov.im/about-the-government/offices/attorney-generals-chambers/

[23] Financial Crime Unit (FCU), https://www.iompolice.im/footer/corporate/financial-crime-unit/

116. The IoM is an international financial centre with large insurance and banking sectors. Online gambling and TCSPs also play an important role in the IoM's non-financial sector. The IoM is also a centre for company formation, and runs successful aircraft and shipping registers. Financial services account for 37% of the Isle of Man's GDP and 32.86% of total employment in the economy. Financial flows into, and out of, the Isle of Man are not measured, but will be numbered in billions of pounds each year.

117. As at 31 March 2016, a total of 237 institutions held a licence issued by the IOMFSA under section 7 of the FSA 2008[24]. The classes of regulated activity which these institutions were permitted to conduct were as follows:

Activity	Number
Deposit Taking (Class 1) (excluding Kaupthing Singer & Friedlander (Isle of Man) Limited, in liquidation)	21
Investment Business (Class 2)	49
Services to Collective Investment Schemes (Class 3)	55
Corporate Services (Class 4)	164
Trust Services (Class 5)	115
Money Transmission Services (Class 8)	5

118. As at 31 March 2016, a total of 198 institutions held a licence issued by the IOMFSA under the IA 2008.

Activity	Number
Life Insurers	16
Non-Life Insurers	118
Foreign Life Insurers[25]	9
Foreign Non-Life Insurers	9
Insurance Managers	22
General Insurance Intermediaries	24

119. As at 31 March 2016, a total of 56 corporate and in house administrators held a registration issued by the IOMFSA under section 36 of the RBS Act 2000. At the same date, a total of 961 retirement benefits schemes were registered as authorised.

120. As at 7 July 2016[26], a total of 322 FIs and DNFBPs had registered with the IOMFSA under the DBRO Act 2015.

Activity	Number
Accountant	152
Lawyer	42
Money Lender	56
Estate Agent	20
Virtual Currency	11
Payroll (stand-alone)	17
Tax Advisor (stand-alone)	15
Specified NPO (SPNO)	6
Other	3

121. In recent years, the insurance and pensions sector has overtaken the banking sector to become the largest single financial sector contributor to the IoM's GDP (£63.9 billion at December 2014 under management and 16% of GDP). The online gambling sector is the largest non-financial

[24] Some licence holders are permitted to conduct more than one class of regulated activity; hence the total in the table (410) exceeds the number of licence holders.

[25] Insurers that also carry on business in a country other than the IoM in accordance with the laws of that country.

[26] Registration of FIs and DNFBPs under the DBRO Act 2015 had not been completed at 31 March 2016. The later date provides a more accurate reflection of the size of the sector regulated under the DBRO Act 2015.

contributor. The life sector represents 88% of the insurance and pension sectors in terms of assets under management. Business in the insurance sector is predominately sourced from the UK (British expatriates) and products are distributed through overseas IFAs. Over 99.5% of policyholder liabilities are attributable to unit-linked insurance products where the benefit payable to the policy-holder on termination is linked to the value of an investment portfolio selected by the policyholder.

122. Life assurance companies are predominately subsidiaries of large internationally active groups headquartered within Europe, mainly the UK. There are a small number of independently owned life assurers in the IoM, and one IoM headquartered listed group, the main entity of which is an IoM life assurance company.

123. The banking sector is the second largest part of the IoM's GDP (deposits of £53 billion at December 2014 and 9% of GDP) but considered to be the sector of greatest significance by the authorities. Whilst banks provide products and services to local customers and businesses (including professional firms), their customer base is predominantly non-resident directly and through third parties (intermediaries). The range of products and services offered is not complex, and includes savings accounts, lending, and some treasury and foreign currency services. Private banking services are offered. All except one bank is part of a group headquartered overseas (mostly in the UK).

124. The securities sector forms a smaller part of the IoM financial services sector (£28bn and 1% of GDP) and is considered to be a less significant component of the financial sector by the authorities. With the exception of financial advisors, the customer base is substantially non-resident (UK-based).

125. The sector manages wealth (trading in securities, advice on investments and management of investments) and administers around 340 funds, the vast majority of which are non-retail (mainly "exempt"[27] and overseas funds). "Exempt" funds are not regulated or supervised by the IOMFSA, and there is no requirement for such funds to be managed or administered in the IoM. There is a single fund "platform" provider.

126. Other financial sector activities, including lending, currency exchange, money transmission, and payment service providers are limited. The customer base for foreign exchange and money transmission is predominantly resident (including migrant workers mainly from European countries).

127. The player base in online casinos gambling is very large and global money deposited at any given time has fluctuated between £250 million and £500 million. The sector accounts for 16.7% of GDP, as of 2013/14, a figure that is still growing. However, employment in online gambling operators (857) accounts for just 2.48% of the private sector. The majority of online gambling operators are privately-owned.

128. The IoM also has a small terrestrial casino whose customer base is predominantly IoM-resident.

129. TCSPs administer around 30,000 client companies and some 20,000 trusts – many of which will be established outside the IoM - but contribute relatively little to GDP (3%) distorted by profits generated by the online gambling and insurance sectors. The TCSP sector is considered by the authorities to be a significant sector[28] (third after banking and insurance and pensions) and to present the highest ML risk (medium-high). Most customers are non-resident and many have a high net worth. TCSPs are predominantly privately-owned, and include some international businesses with large numbers of employees.

[27] "Exempt" funds are private arrangements that can have no more than 50 investors, and whose constitutional documents must expressly prohibit the making of an invitation to the public to subscribe in any part of the world.

[28] Based on consideration of 5 factors: (i) assets under management; (ii) capital flow; (iii) income; (iv) employment; and (v) GDP contribution.

130. Structures established for customers can also be complex and can be established for trading purposes. However, most business in the IoM is "fully managed" - with TCSP staff acting as directors or trustees. Accordingly, "registered office only" business is not common and "mixed boards" are rare.

131. Lawyers practice criminal, family, property and corporate and commercial law and are self-regulated by the IoM Law Society (except for AML/CFT purposes where they are regulated and supervised by the IOMFSA). Around a third of law firms have an international client base with the remainder largely offering conveyancing services to IoM residents. Foreign lawyers (registered legal practitioners) can also practice in the IoM. Whilst a number of practices provide TCSP services, they do so through separately licenced TCSPs. Operators in this sector range in size from sole practitioners to the IoM partnership of an international practice.

132. Accountants offer audit, tax and advisory (transactions) services only and are not generally involved in property transactions. Very few accountancy firms hold client accounts. Whilst a number of practices provide TCSP services, they do so through separately licenced TCSPs. Tax services focus on compliance with legislation, rather than providing advice on structures and mitigation of tax liabilities. This type of advice is provided by lawyers and accountants outside the IoM or in-house specialists employed by TCSPs. Operators in this sector range in size from sole practitioners to IoM offices of large international practices.

133. The role of estate agents is limited to facilitation of sales transactions between sellers and buyers. Transactions relating to sale, the transfer of ownership and payment are conducted by lawyers. Whilst there is a limited high-end housing market in the IoM, an on-going case demonstrates that Manx real estate can be used to launder criminal proceeds.

134. Like many jurisdictions, the IoM is looking to develop its "FinTech" industry and growth in this sector could be significant. It is not thought that convertible virtual currencies will contribute significantly to this growth.

135. Given the predominantly non-face-to-face and cross-border nature of the financial sector and work undertaken by DNFBPs, extensive use is made by banks and TCSPs of CDD measures applied by third parties. In contrast, life assurance companies delegate the collection of CDD measures to IFAs – in accordance with terms of business between the assurance company and IFA.

Overview of preventive measures

136. Section 157(1) of the Proceeds of Crime Act 2008 provides that the Department of Home Affairs must make such codes as it considers appropriate for the purposes of preventing and detecting money laundering. There is a similar provision in the Terrorism (Finance) Act 2009. A number of money laundering and terrorist financing codes have been made under these provisions. These were combined into a single set of Codes in 2013 – the AML/CFT Code - and most recently amended on 1 April 2015. The AML/CFT Code applies to all FIs and DNFBPs.

137. In order to assist FIs and DNFBPs (excluding online gambling operators) comply with the AML/CFT Code, the IOMFSA also publishes guidance in the form of an AML/CFT Handbook (not "enforceable means") which is supplemented by sector specific guidance.

138. In addition to the AML/CFT Codes, life (and non-life) insurers are subject also to a set of insurance-related AML/CFT requirements in the form of the Insurance Anti-Money Laundering Regulations 2008 ("IAMLR"). These Regulations were last revised in 2008 and are supported by guidance set out in the Insurance Guidance Notes which, despite their name, are enforceable means for the purposes of the FATF Recommendations.

139. A separate code - the Money Laundering and Terrorist Financing (Online Gambling) Code 2013 ("Online Gambling Code") - applies to online gambling operators. This Code was last revised in 2013. The Online Gambling Code is supported by guidance published by the GSC.

140. In addition, FIs and DNFBPs are required to report suspicious transactions relating to funds that are suspected to be: (i) the proceeds of criminal activity - under the Proceeds of Crime Act 2008 (Sections 142 to 144, and 153 to 154); and (ii) related to terrorism financing - Anti-Terrorism and Crime Act 2003 (Sections 11, 12, 14 and 15).

Risk-based exemptions or extension of preventative measures

141. In cases where a customer acts on behalf of another person, paragraph 21 of the AML/CFT Code has exempted some FIs from the requirement to identify upfront that other person, and take reasonable measures to verify that other person's identity (provided a number of conditions specified in this Code paragraph are met). The exemptions provided under paragraph 21 of the AML/CFT Code are mainly based on the fact that the customer is subject to requirements to combat ML/TF consistent with the FATF Recommendations and has effectively implemented those requirements, but does not fully take into account other risk factors and variables mentioned in the Interpretative Note to R.10, most importantly when it comes to the risk profile of the underlying clients. Similarly, paragraphs 20, 22 and 24, of the AML/CFT Code exempt some FIs and DNFBPs from taking measures to verify the identity of a customer in permitted circumstances. Most are based on the examples provided in the Interpretive Note to Recommendation 10, paragraph 17(a) and (b) and it appears that the authorities have based their conclusions on their supervisory experience. Some deficiencies in the application of exemptions are highlighted under c.1.6 and c.10.5. Risks inherent in the application of these exemptions were not considered in the NRA.

142. The AML/CFT Code applies also to: (i) the non-life insurance sector (assessed in the NRA as presenting a medium low vulnerability), including captives, general insurance brokers and insurance managers; (ii) pension providers (assessed in the NRA as presenting a medium risk), including occupational schemes; (iii) betting shops and controlled machine suppliers (Not assessed in the NRA on the grounds that the domestic gambling sector is "less useful to criminals seeking to launder large volumes of money". The number of these shops and suppliers is very small); (iv) payroll agents (not assessed in the NRA - but will be considered at a later point in time). (v) The land based casino.

143. Most recently, application of the AML/CFT Code has been extended to include convertible virtual currency operators in response to: (i) promotion of this sector by the IoM Government; and (ii) emerging consensus on the risks that are inherent in the use of convertible virtual currencies.

Overview of legal persons and arrangements

Legal persons

144. The types of legal person that can be established in the Isle of Man are: (i) companies incorporated under the Companies Act 1931 to 2004 ("1931 company"); (ii) companies incorporated under the Companies Act 2006 ("2006 company"); (iii) limited liability companies ("LLCs") incorporated under the Limited Liability Companies Act 1996; (iv) limited partnerships with legal personality incorporated under the Partnership Act 1909; (v) foundations established under the Foundations Act 2011; and (vi) industrial and building societies established under the Industrial and Building Societies Acts 1892 to 1979.

145. 1931 and 2006 companies can also be established as a protected cell company, an incorporated cell company, or an incorporated cell.

146. The legal status of 1931 companies and 2006 companies is the same: they are incorporated, have a legal personality separate from their members, and day to day management is conducted through directors. In the case of a company limited by shares or guarantee, liability of members is limited to their contribution of capital or amount guaranteed. 2006 companies are described as simplified corporate vehicles and not subject to a number of traditional company law formalities, such as: (i) the requirement to hold an annual general meeting; (ii) the requirement to appoint a company secretary; and (iii) a number of registry filings. Each 2006 company must have a registered

agent in the IoM (a TCSP that is regulated and supervised by the IOMFSA) who is one of the key people responsible for ensuring that it is properly administered.

147. LLCs have only members and are a form of incorporated partnership. Management of a LLC is vested in the members in proportion to their contribution of capital. The profits of the company are treated as income of the members. Each LLC must have a registered agent in the IoM (likely to be a TCSP that is regulated and supervised by the IOMFSA).

148. Whilst having much in common with a trust, a foundation is incorporated and has a distinct legal personality, something more commonly associated with companies. Each foundation must have a registered agent in the IoM (a TCSP that is regulated and supervised by the IOMFSA).

149. In addition, partnerships, including limited partnerships, are established under the Partnership Act 1909 and may not generally consist of more than 20 members (though there are some important exceptions, e.g. advocates, accountants and regulated collective investment schemes). The assets of a partnership are jointly owned by the partners and must be held and applied exclusively for the partnership and in accordance with the partnership agreement. On this basis, they are considered to be legal persons (as defined by the FATF).

150. A limited partnership is a partnership that is registered under the Act and must consist of: (i) at least one general partner, who manages the partnership and is responsible for all of its debts and obligations; (ii) at least one limited partner (similar to a shareholder), who invests a defined amount of capital and liable only for debts of the partnership up to the amount contributed. A limited partner cannot be involved in day to day management, except as provided for in the Act. A limited partnership may have a legal personality if the general partners so elect at the time that the partnership is registered. A partnership is not a taxable entity, and so each partner is liable to pay tax on their share of profits.

151. Partnerships are required to maintain a place of business in the IoM, though there is no requirement to keep beneficial ownership information at that address.

152. An application to form a foundation may be made only by a registered agent in the IoM (a TCSP that is regulated and supervised by the IOMFSA). There is no similar restriction on who may apply to form other types of legal person.

153. All companies and foundations must be registered with the Central Registry. A partnership cannot become a limited partnership if it does not register with the Central Registry. General partnerships are not required to be registered with the Central Registry. The Central Registry is responsible for administering each of the laws referred to above, which includes enforcing payment of fees and submission of annual returns or statements (all companies, foundations and limited partnerships). Late filing fees are applied if returns or statements are delivered late. Failure to file an annual return or statement can result in a company or limited partnership being struck-off the register (but not also a foundation).

154. Table 1 below shows the number of legal persons registered with the Central Registry between 2011 and 2015.

Legal person	**2015**	**2014**	**2013**	**2012**	**2011**
1931 companies	19,437	19,302	20,047	21,215	22,333
2006 companies	9,139	8,792	8,355	7,396	6,542
LLCs	249	218	235	248	276
Foundations	62	52	35	17	0
Limited partnerships	280	269	291	N/A	N/A
General partnerships	N/A	N/A	N/A	N/A	N/A
Industrial societies	6	6	6	6	6

155. 2006 companies tend to be used now by non-residents, and this accounts for the gradual decline in the number of "live" 1931 companies and increase in 2006 companies. Many 2006 companies are used to hold property for their beneficial owner. Data provided for dissolved companies for the period from 2000 to 2009 shows that those companies spent an average of 5 years on the register.

156. The authorities advise that because companies (except 1931 companies) and foundations are required to appoint registered agents, the majority of legal persons in the IoM are administered by TCSPs. TCSPs also provide all of the services to third parties that are listed in the FATF definition of TCSP. A TCSP is required to apply CDD measures to its customer(s) (and beneficial owner(s)) in accordance with the AML/CFT Code.[29] CSPs have been regulated and supervised in the Isle of Man since 2000 and TSPs since 2005. Unlike in many other jurisdictions, regulation is not limited to compliance only with AML/CFT legislation, and extends to prudential matters and conduct of business (including "fit and proper" testing of controllers, directors and "key persons"). The FSA (and its predecessor) also proactively supervises the sector for AML/CFT compliance.

157. Companies, foundations and limited partnerships must comply with a requirement to file annual returns. Except in the case of 2006 companies, these returns must present basic information, including names and addresses of directors or equivalent and registered office on the anniversary of its registration. There is also a requirement to notify the Central Registry about any prescribed changes to information, generally within one month of the change occurring. The Central Registry may undertake enforcement action against companies that fail to file annual returns or deliver prescribed information late. A company that fails to deliver its annual return can also be struck off the register.

158. The IoM does not currently hold beneficial ownership information centrally, though it is committed to doing so by 2017.

Legal arrangements

159. Trusts in the IoM are governed by common law and the Trusts Act 1995. Whilst it is not possible to estimate how many trusts are governed by Manx law, approximately 19,000 trusts are administered by TCSPs in the IoM (though not all will be governed by Manx law).

160. Where created in the IoM, trusts will usually be established by TCSPs or lawyers. There are no explicit obligations in the Trusts Act 1995 for trustees to keep accurate and up to date information in relation to trusts, though trustees are subject to the duty to account to the beneficiaries. Where a trust has professional trustees in the IoM, when acting in that capacity, they are subject to the AML/CFT Code. Section 13 of the AML/CFT Code explains that, inter alia, CDD measures must be applied to known beneficiaries, settlors and any person who is able to direct the trust's activities. Additional information is provided in sector specific guidance notes for TCSPs published by the IOMFSA in December 2015.

International context for legal persons and legal arrangements

161. Except in the case of 1931 companies, the vast majority of beneficial owners of legal persons and legal arrangements established under Manx legislation are non-residents. Accordingly, the authorities receive and respond to a large number of requests each year from overseas counterparts which involve the use of Manx legal persons and legal arrangements. The FIU estimates that around 50% of requests that it receives are for intelligence in respect of Manx legal persons and legal arrangements and data provided by the Income Tax Department shows that a similar percentage of requests for beneficial ownership information relates to corporate entities and trusts. The IOMFSA has explained that almost half of the requests that is receives for beneficial ownership information include companies. And round 25% of requests for MLA received by the AGC involve the collection of

[29] A registered agent is given a number of legal responsibilities, e.g. holding documents and records and filing statutory returns and is responsible for ensuring that a legal person is properly administered.

information from TCSPs. The authorities say that they have never received a complaint or supplementary request for information on the basis that information provided was missing or inaccurate.

162. Management information on the countries in which beneficial owners of legal persons and legal arrangements are resident is not held by the authorities. However, the authorities report that there is extensive use made of IoM companies to hold real estate in London, and the IOMFSA has explained that almost two-thirds of the requests that it receives for beneficial ownership information come from supervisors in the UK or US.

Overview of supervisory arrangements

163. In the IoM, FIs and DNFBPs (except casinos and online gambling) are regulated and supervised by the IOMFSA for AML/CFT purposes. The IOMFSA supervises banks, securities firms, operators of collective investment schemes, TCSPs and MSBs under the Financial Services Act ("FSA") 2008, and life assurance companies (and other insurance and pension activities) are supervised under the Insurance Act 2008 and pension activities under the Retirement Benefits Schemes Act 2000. The IOMFSA also supervises collective investment schemes under the Collective Investments Schemes Act 2008 for AML/CFT purposes.

164. Other FIs and DNFBPs are supervised under the Designated Business (Registration and Oversight) Act 2015 ("DBRO Act"), which came into force in October 2015. Up until this time, the Law Society of the IoM and five UK accountancy bodies (including the Institute of Chartered Accountants in England and Wales and Association of Chartered Certified Accountants) had responsibility for monitoring compliance by their members in the IoM with the AML/CFT Code under memoranda of understanding in place with the Department for Home Affairs. The late introduction of specific measures to supervise AML/CFT compliance by FIs and DNFBPs not otherwise overseen by the IOMFSA, GSC, Law Society of the IoM or UK accountancy bodies has an impact on this assessment, most notably on IO.3.

165. Under arrangements now in place with the IOMFSA, the Law Society and UK accountancy bodies can continue to supervise their members under the DBRO Act, on behalf of the IOMFSA. However, only the IOMFSA has the power to take enforcement action under this law.

166. The IOMFSA was established in 2015, as a result of a merger between the Financial Supervision Commission ("FSC") and the Insurance and Pensions Authority. Its regulatory objectives include reduction of financial crime. It has a broad range of powers to supervise and monitor compliance with AML/CFT requirements, including powers of off-site reviews and analysis and on-site inspection visits.

167. Persons carrying on, or providing, particular types of: (i) investment business; (ii) corporate services; (iii) trust services; (iv) deposit-taking; or (v) services to collective investment schemes, that are exempted by the Financial Services (Exemptions) Regulations 2011 are not required to be licenced by the IOMFSA (though they are otherwise subject to regulation and supervision, including compliance with AML/CFT requirements). The latter category includes persons acting as director for up to 10 companies and a single purpose manager of an exempt fund.

168. The GSC supervises terrestrial casinos and online gambling for AML/CFT purposes. The scope of its regulatory and supervisory remit is wider than casinos. Its regulatory objectives include preventing gambling from being a source of crime or disorder, associated with crime or disorder, or used to support crime. Casinos are regulated under the Casino Act 1986 and online gambling under the Online Gambling Regulation Act 2001.

169. The GSC has a broad range of powers to supervise and monitor compliance of online gambling operators and the IoM's only terrestrial casino with the Online Gambling Code and AML/CFT Code respectively, including powers of off-site reviews and analysis and on-site inspection visits.

However, these AML/CFT oversight powers are reliant on licensing conditions a fact which is identified by the NRA.

CHAPTER 2. NATIONAL AML/CFT POLICIES AND COORDINATION

Key Findings and Recommended Actions

Key Findings

• The IoM has made significant efforts to understand its ML/FT risks, especially by conducting a formal NRA process.

• The assessment of institutional vulnerabilities was thorough, which resulted in the identification of important gaps in the national system and corresponding risk mitigation measures. The vulnerabilities within the financial and non-financial sector are broadly understood although some areas appear not to have been subject to a sufficiently detailed analysis. For instance, the risk resulting from the use by banks of CDD information provided by TCSPs that have collected this information in turn from a professional intermediary is not fully understood. The vulnerability of lawyers and the real estate sector appears to have been underrated, as has the risk associated with border controls.

• The authorities understand that the ML threats are mainly external. Various factors were analysed in order to form a conclusion on cross-border threats, such as data based on sectorial information, SARs and MLA requests. However, the understanding of the external threat is restricted by the absence of aggregate data on the volume and destination of outgoing and incoming flows of funds in the financial sector and lack of aggregated information on where the beneficial owners of assets managed or held in the IoM are from.

• The NRA looks at the FT threat from various angles with well-considered conclusions. However, there is an important element which is missing. An assessment of the flows leaving the IoM, which could potentially be linked to the financing of terrorism, terrorist groups or individual terrorists in other countries, especially in high-risk jurisdictions, has not been carried out.

• The IoM has taken prompt action to mitigate the risks identified in the NRA. An action plan was drafted following the publication of the NRA. The action plan addresses all the issues identified in the NRA. Many actions had already been implemented at the time of the on-site visit, while others were still on-going.

• The results of the NRA have not yet been used to support the application of exemptions, enhanced measures for higher risk scenarios and limited simplified measures for lower risk scenarios. The FIU and law enforcement authorities are in the process of implementing their objectives and activities in line with the identified risks. Although the activities of the IOMFSA are to some extent in line with the risks present in the country, there is an over-focus on the risks posed by individual institutions rather than the different sectors as a whole. The GSC's objectives and activities have been adjusted to take into consideration the risks identified in the NRA.

• There are many positive aspects in the mechanism for national co-operation and co-ordination of AML/CFT policies and activities. The AML/CFT Strategic Group prioritises issues of importance for the national AML/CFT policy. Its work is complemented by that of the AML/CFT Technical Group, which put forward many proposals for the improvement of the national framework. Most competent authorities co-ordinate their activities at an operational level. However, there are some areas which require further improvement, such as the implementation of TFS, the investigation of FT and the control of borders for the detection of non-declared or falsely declared cash.

• The AML/CFT Strategic Group is entrusted with the co-ordination of policies and activities concerning PF. However, a formal action protocol is missing to formalise co-operation arrangements

between all the relevant agencies and clearly provide a framework for the different agencies' responsibilities in PF activities.

Recommended Actions

• As identified in the NRA the authorities should take steps to collect statistics on outgoing and incoming flows of funds in the financial sector. The IoM should then conduct a reassessment of those areas which would have benefitted from these statistics, mainly cross-border ML and FT threats.

• The authorities should seek to understand where the beneficial owners of assets managed or held by regulated entities in the IoM are from and consider this information in the next iteration of the NRA.

• The IoM should undertake a more detailed assessment of the risk resulting from the use by banks of CDD information provided by TCSPs that have collected this information in turn from a professional intermediary. The authorities should also consider re-assessing the risk posed by lawyers, the real estate sector and the threat posed by cash entering and exiting the IoM.

• The IoM should consider whether the exemptions, higher risk scenarios and lower risk scenarios, which support the application of enhanced and simplified measures respectively, set out in the AML/CFT Code, are consistent with the ML/FT risks present in the country.

• Going forward, it should be ensured that the objectives and activities of the FIU and LEAs are consistent with AML/CFT policies and the identified ML/FT risks.

• The authorities should introduce (or strengthen existing ones, as the case may be) co-operation mechanisms in those areas which are identified as missing in this report, including a formal PF policy.

The relevant Immediate Outcome considered and assessed in this chapter is IO1. The recommendations relevant for the assessment of effectiveness under this section are R1-2.

Immediate Outcome 1 (Risk, Policy and Coordination)

Country's understanding of its ML/TF risks

170. The NRA accurately reflects and represents the authorities' understanding of ML/FT risks facing the IoM. The authorities endeavoured to conduct a candid assessment of the institutional vulnerabilities, which has resulted in the identification of important gaps in the national system. This has enabled the authorities to undertake a number of targeted measures and allocate resources where needed.

171. The vulnerabilities within the financial and DNFBP sub-sectors are broadly understood. The authorities are well aware of where the main risks lie within the private sector. The NRA process entailed a detailed analysis of the types of products, services, geographical links and delivery channels which feature in the IoM. This has enabled the authorities to form a view of the nature of the business and the inherent vulnerabilities within the system.

172. The authorities understand that the TCSP sector, given its significant presence, increases the IoM's inherent vulnerability to ML/FT risks. It is acknowledged that business introduced by professional intermediaries, e.g. TCSPs, increases the inherent risks to banks and other FIs and DNFBPs that make use of CDD applied by such third parties. For example, with a view to mitigating these risks, specific requirements have been introduced within the AML/CFT Code, which are referred to as eligible introducer (reliance) provisions. However, the authorities have not conducted a complete assessment to determine the degree to which use is made of professional intermediaries to collect CDD information and evidence, including under eligible introducer provisions, in practice, although extensive on-site work has been conducted by the IOMFSA assessing banks' procedures and approach to accepting business from TCSPs. It is therefore unlikely that the cumulative risk

resulting from the interaction between the banking and the TCSP sector is comprehensively addressed. In particular, the extent to which CDD information provided to banks by TCSPs has in turn been provided to the TCSP by a professional intermediary is not known. Where there are such "information chains", the using information provided by the TCSP, may be given incomplete or false information and so unable to understand the nature of the customer's business and its ownership and control structure. The situation is exacerbated by the fact that TCSPs met on-site appeared to downplay the level of risk to which their sector is exposed.

173. As stated in Chapter 1, a number of indicators were considered in the NRA to determine the level of ML/FT threat. The authorities recognise that the ML/FT threats to the IoM are predominantly external, particularly coming from the UK, where most of the business originates. This understanding is facilitated by long-standing and thorough supervision (including on-site visit programme and access to SARs) over most of the sectors. However, there are two factors which appear to militate against a complete understanding of external threats. The first is the absence of data collected nationally on the aggregate volume and destination of outgoing and incoming flows of funds in the financial sector (this is acknowledged in the NRA and measures were already being taken at the time of the on-site visit to address this issue). Secondly, although the IoM is a centre with a large non-resident customer base, the authorities do not have aggregated information on the beneficial owners of assets managed or funds held by IoM financial institutions and DNFBPs or know which countries those funds are coming from and going to.

174. The NRA considers the FT threat from various angles, with well-considered conclusions. However, it does not assess the threat of the IoM being used as a conduit for financial flows intended to finance terrorism, terrorist groups or individual terrorists in other countries, especially in areas of conflict. The authorities are of the view that, should such cases have ever materialised, it is likely these would have been brought to their attention by the UK intelligence services. Due to the constitutional position of the IoM, some reliance on the UK with respect to defence and security matters is inevitable.

175. The evaluation team does not share the conclusions of the NRA with respect to the lower risk rating awarded to lawyers and the real estate sector. The evaluators were made aware of cases where ML on the IoM may have been facilitated by lawyers (whether wittingly or unwittingly), including through the use of pooled accounts. Additionally, there were cases where real estate was purchased using the proceeds of criminality. However, not all of this information was available or, where it was available, fed into the NRA process, which could have assisted the authorities in reaching a more balanced conclusion. This area was already under review at the time of the on-site visit, as a new DNFBP supervisory regime was being implemented and, as a result, more detailed data and information on these sectors was being gathered.

176. The NRA does not assess the threat of cash entering into the IoM. It is stated that there is evidence to support the view that it has become much more difficult in recent years to place illicit cash directly into banks or other institutions. However, due to limited controls on cash movements, this conclusion is not supported by complete information It should also be noted that the UK's NRA identifies cash-couriering as a high risk, which could have an impact on the risk faced by the IoM, since there are no borders and cash may be freely transported from the UK into the IoM. This has also not been considered. The NRA only states that the UK does not regard the IoM as a significant cash courier risk.

National policies to address identified ML/TF risks

177. Following the publication of the NRA in June 2015, the IoM adopted an action plan to address the identified ML/FT risks, threats and vulnerabilities. The AML/CFT Strategic Group is responsible for the implementation of the action plan. The evaluation team was satisfied that the measures implemented by the IoM address the identified risks.

178. The top three prioritised actions identified by the NRA Tool at national level were data collection and coordination, financial crime investigation and financial intelligence gathering and processing. Measures to address these issues were undertaken immediately upon the completion of the NRA, some of which were still on-going at the time of the on-site visit. The FCU undertook a training needs assessment which identified a need to set a minimum accreditation requirement of investigators and to provide bespoke training for handling financial intelligence and financial investigations. The resources of the FCU were also increased. A new FIU Act was enacted in April 2016, providing for the establishment of an autonomous unit with all the powers and functions required under the FATF Standards. Measures were taken to operationally separate the FIU and financial crime investigations, with a new interim Director of the FIU (a retired senior Police Officer) being appointed in October 2015. The Cabinet Office was in the process of developing an overall Government approach to data collection. This involves coordination with all relevant authorities on the IoM.

179. Measures to strengthen the regulatory and preventive regime, as a means to address private sector vulnerabilities, were also undertaken. For instance, civil penalty regulations were enacted to reinforce the sanctioning mechanism, a new desk-based return covering certain AML/CFT matters was adopted, and feedback was issued to the private sector on the monitoring of higher or increased risk matters.

Exemptions, enhanced and simplified measures

180. Requirements in the AML/CFT Code and Online Gambling Code apply to all business conducted in the regulated sector (defined in Schedule 4 of the POCA 2008). Indeed, it goes beyond the FATF Standards by including certain entities, such as payroll agents, within its scope. However, where certain FIs determine that a customer is acting on behalf of another person, paragraph 21 of the AML/CFT Code exempts those FIs from requirements to: (i) identify that other person; and (ii) take reasonable measures to verify that other person's identity, in permitted circumstances. The exemptions provided under paragraph21 of the AML/CFT Code are mainly based on the fact that the customer is subject to requirements to combat ML/TF consistent with the FATF Recommendations and has effectively implemented those requirements, but does not fully take into account other risk factors and variables mentioned in the Interpretative Note to R.10, most importantly when it comes to the risk profile of the underlying clients. Similarly, paragraphs 20, 22 and 24, of the AML/CFT Code exempt FIs and DNFBPs from taking measures to verify the identity of a customer in permitted circumstances. Risks inherent in the application of these exemptions in section 21 have not been considered in the NRA or other risk assessment. Most are based on the examples provided in the Interpretive Note to Recommendation 10, paragraph 17(a) and (b) and it appears that the authorities have based their conclusions on their supervisory experience. Some deficiencies in the application of exemptions are highlighted under c.1.6 and c.10.5.

181. The AML/CFT Code also permits reporting entities to apply simplified CDD in cases where the risk is low (though the AML/CFT Handbook says that this may be in exceptional circumstances and where certain conditions are met only) and no suspicious activity has been identified. However, no risk assessment was carried out with respect to the cases where the application of simplified CDD is possible.

182. Reporting entities are required to apply enhanced measures in higher risk situations. However, as noted under Criterion 10.17, the present AML/CFT Code came into force before the NRA was completed and the relevant provisions dealing with enhanced CDD have not yet been updated (as appropriate) to take account of risks identified.

Objectives and activities of competent authorities

183. The IOMFSA's policies and actions are to some extent consistent with the NRA and risks identified in the IoM. However, as noted under IO.3, the IOMFSA does not routinely collect and aggregate information across all sectors on customer risk classifications, numbers of PEPs, residence of beneficial owners of customers, or extent to which exemptions or simplified CDD measures are applied under the AML/CFT Code. And, whereas the NRA considers and assesses the ML/TF risk of each financial sector, the IOMFSA does not currently identify and maintain an understanding of the ML/TF risk between different sectors and type of institution, or allocate resources based on such an understanding. Instead, its focus is on risk assessments of individual FIs and DNFBPs. It is not clear how it considers whether overall ML/TF risk rating spreads are consistent with sectorial analyses of risk in the NRA. The IOMFSA does not provide sufficient attention to the extent to which banks use CDD information presented by TCSPs that have collected this information in turn from other parties. The IOMFSA's objectives, consistent with the risks posed by DNFBPs, were being shaped at the time of the on-site visit, as the IOMFSA was still in the process of collecting information from DNFBPs as part of the new supervisory structure set up under the DBRO.

184. Following the completion of the NRA, the GSC's understanding of risks improved considerably. At the time of the on-site visit, its objectives had already been adjusted to take into account the risks identified.

185. It is unclear how the FIU prioritises its objectives and activities and how these are commensurate to the risks identified. The main focus currently lies on developing and improving its financial analysis regime in line with the findings of the NRA. It was not demonstrated to the satisfaction of the evaluation team that the FIU prioritises its work according to, for instance, cases which involve ML with a foreign predicate offence or cases involving complex trust and corporate structures.

186. Law enforcement action (including CED) is mainly focussed on domestic predicate offending, but is not commensurate with the ML risk emanating from these and other types of offenses, especially those committed abroad. However, there has been a recent focussing on ML investigations involving foreign predicate offences. It is anticipated that the outcome of the recognised need to interrogate the product of incoming MLA requests will lead to more investigations into ML where the predicate offence is outside the IoM. Liaison between the FIU and LEA through the Joint Tasking Group has identified this outcome as a likely demand driver in future.

National coordination and cooperation

187. Given the size of the IoM, the authorities co-operate and co-ordinate the development of policies and activities to combat ML/FT to a large extent.

188. The AML/CFT Strategic Group takes the lead in this area. The assessment team had sight of the minutes of the meetings of the Strategic Group`s which amply demonstrate that it prioritises issues of importance for the national AML/CFT policy.

189. The work of the AML/CFT Strategic Group is complemented by the AML/CFT Technical Group, which is responsible for implementing the high-level decisions taken by the Strategic Group. Its functions include: enabling cooperation and coordination of activities between competent authorities and others, including FIs; providing information and advice to the Strategic Group on relevant matters, including on actions and recommendations arising out of international assessments, conventions and protocols etc.; monitoring and reporting on progress against international recommendations; and participating in and contributing to the NRA process.

190. At an operational level, the FCU, the FIU, the CED and the ITD cooperate closely when investigating financial crime. Information and intelligence flows between the different authorities without any restrictions, either in law or in practice. Joint and co-operative investigations between

different competent authorities such as the FCU and the CED have occurred. The evaluation team was also satisfied that the IOMFSA cooperates closely with LEAs when the need arises. For instances examples where provided where the IOMFSA took regulatory action as a result of information provided by the FCU.

191. However, the evaluation team identified areas where operational co-operation and co-ordination between the various competent authorities could be improved. These are referred to in various chapters of this report. For instance, while some form of co-operation exists between the IOMFSA and the CED regarding the implementation of international financial sanctions, the mechanism in place is not holistic. The exchange of information between the relevant authorities involved in prevention and detection of TF does not always occur, and in many cases information held by the CED, the FIU, the IOMFSA or the police, regarding potential FT suspicion is not made available to the other relevant competent authorities. There seems to be a lack of an overarching policy between the Police and the CED for the detection of falsely or undeclared cross-border movements of currency and bearer negotiable instruments, which results in a lack of policy regarding confiscation of these, if detected.

192. The AML/CFT Strategic Group also co-ordinates policymaking and provides a platform for co-operation between the domestic authorities. The authorities have provided minutes of meetings, but the PF policy issues have been raised only in some occasions and no major PF co-operation issues were discussed. While the authorities have provided examples of co-ordination and co-operation, it has not been sufficient enough as elaborated further under IO 11. A formal action protocol that formalises co-operation arrangements between all the relevant agencies and clearly provides a framework of different agencies' responsibilities in PF-activities is missing. This protocol would increase the awareness, in both the public and private sector, and encourage businesses to bear in mind PF-risks and how to report any concerns, suspicions, etc. Consequently, the protocol can be the cornerstone for future enhancements, something which the authorities acknowledge.

Communication of risks to the private sector

193. The private sector was involved in the NRA process from its earliest stages, with one sector module working group being co-chaired by a representative from the private sector. In particular, representatives from banking, insurance and pensions and securities were significantly involved in the process, although all sectors were engaged at some point. The private sector representatives met on-site demonstrated a general understanding of the risks identified in the NRA and confirmed that the authorities had sufficiently communicated the sector-specific outcomes of the NRA.

194. The feedback provided by the authorities varied depending upon the requirements of the sector. It included detailed written feedback from the NRA sector report/s; conferences, presentations and workshops; meetings with representatives of professional and industry bodies and one-to-one meetings. In some cases, the feedback was sent jointly by the Cabinet Office and relevant regulator directly; in other cases, the correspondence forwarded to members by and with the agreement of the professional or industry body.

Conclusion

195. In determining the rating for IO 1, the evaluation took into consideration the fact that the IoM has made significant efforts to understand the ML/FT risks it faces and has a strong national co-ordination mechanism. The NRA process, which was a multi-stakeholder exercise, was conducted very diligently and transparently by the authorities, backed by political commitment at the highest level. Where data and information was missing, this was acknowledged in the NRA document itself. Efforts were made to minimise the impact on risk understanding resulting from information gaps. Besides the NRA, the understanding of vulnerabilities within the financial sector (including TCSPs) is supported by years of supervisory experience. The evaluation team was also satisfied that measures

had already been instituted, even before the on-site visit, to address those risks identified in the NRA. There were, however, some areas which were not considered in sufficient depth, such as FT threats, the risks posed by lawyers and the real estate sector and cross-border threats. In these cases, the understanding is not yet comprehensive enough rather than completely missing. The shortcomings in the assessment of the FT threat were given less weight under IO 1 and the consequences of these will be considered further under the analysis of IO 9. **The IoM has achieved a substantial level of effectiveness for IO.1.**

CHAPTER 3. LEGAL SYSTEM AND OPERATIONAL ISSUES

Key Findings and Recommended Actions

Key Findings

Immediate Outcome 6

• Both the FIU and the FCU have access to a wide range of financial, law enforcement and administrative information, which they access regularly. However, during the period under review, although the FIU was empowered to request additional information from reporting entities, it was unable to compel them to provide it without a production order made by the court.

• The FIU assisted the FCU in the course of its ML investigations mainly in obtaining information. Only occasionally did the FIU conduct in-depth analysis and, as a result, the intelligence products of the FIU did not often add significant value. In view of this, FIU analysis and dissemination provided limited support to the operational needs of law enforcement authorities. FIU disseminations have, however, led to the IOMFSA taking regulatory measures with respect to licence holders.

• The profile of the cases dealt with by the FIU does not reflect the risks facing the IoM. The FIU has only rarely handled complex cases involving corporate structures with legal entities and arrangements situated in different jurisdictions.

• The FIU disseminated 6 domestic FT-related intelligence reports that did not result in any FT investigations.

• The types of SARs that the FIU received frequently did not contain sufficient relevant information to assist them in performing their functions. Defensive reporting is still considered to be high. Few SARs actually contain substantial ML/TF suspicions. Improvement in this area is an action point in the NRA. Adequate detailed feedback on reporting is not provided on a regular basis.

• The FIU regularly exchanged information with other law enforcement authorities and the IOMFSA and to a lesser extent with the GSC.

Immediate Outcome 7

• The IoM has a sound legal system with robust AML/CFT legislation mirroring UK legislation. It enjoys an independent judiciary committed to the rule of law. The relevant authorities involved in the detection investigation and prosecution of ML are all skilled and motivated. Further specialised training should be considered. More resources could be applied to the AGC and the police involved in the investigation of financial crime.

• The IoM is a small jurisdiction and thus the on-going interaction amongst all the relevant players is not surprising. It facilitates good informal contacts. Nevertheless, there is a lack of sufficient systematic cooperation and coordination, which could lead to missed opportunities in detecting and investigating ML. Enhanced engagement of the AGC in the investigatory phase may result in more successful and timely indictment of ML offenders and restraint of their assets.

• The criminal justice system effectively detects, investigates and prosecutes criminality affecting domestic security such as fraud, theft and drug crimes, and the corresponding ML offences.

Nevertheless, ML is not sufficiently detected and investigated with regard to suspicion arising from SARs, identified by supervision of FIs and DNFBPs, or by harvesting information from incoming MLA requests. Parallel financial investigations are conducted but not systematically and not in cases where the associated predicate offences occur outside the IoM. These are considered to be material shortcomings in the system in view of the IoM's context.

• The IoM authorities have in the past prosecuted all types of ML cases including self-laundering, third party laundering and stand-alone ML. However, the investigation and prosecution of ML, in recent years, whilst they have been in line with the domestic risks have not been in line with the international risks faced by the IoM, and are over focused on domestic crime predominantly drug or fraud cases with relatively low proceeds. In recent years there have been no third party or stand-alone ML convictions involving complex structures or when used to launder foreign predicate criminality.

• When offenders are successfully prosecuted the courts apply sanctions, though these seem low and not dissuasive.

Immediate Outcome 8

• The IoM legal framework on restraint and confiscation is comprehensive. It provides adequate tools for detection, restraint and confiscation of instrumentalities and proceeds of crime, both for domestic and international criminal cases. It also provides a robust non-conviction based civil recovery regime which goes beyond the FATF standards.

• The authorities do not pursue the confiscation of proceeds of crime as a policy objective. In those cases where the law enforcement agencies are considering applying for confiscation, the legal principle of proportionality is over-relied upon. In some cases, this has led to a situation where not all possible assets have been confiscated. However, in those cases where the prosecution brought forward applications for confiscation orders, the court has considered the evidence submitted by the prosecution and, where satisfied that it was appropriate to do so, made a confiscation order.

• The authorities have restrained and confiscated assets in some international and domestic cases of predicate offences and ML. However, the overall value of property restrained, confiscated, and actually recovered remains extremely low and does not reflect the risks in the IoM.

• The focus is on the restraint and confiscation of proceeds from predicate crime (e.g. drugs, tax and other predicate offences or included in foreign MLA requests). Confiscation of criminal proceeds and instrumentalities of the ML offence, as well as of property of equivalent value are not pursued systematically, especially in cases where the victim of the predicate crime has been compensated.

• The confiscation of cross-border cash and BNIs related to ML/TF/associated predicate offences is not applied in the IoM as an effective, proportionate and dissuasive sanction. The powers to seize falsely or undeclared cash or BNIs for further investigation were utilised on a very limited basis.

• Parallel financial investigations aimed at the detection of potential criminal assets subject to confiscation are not systematically applied.

• There is very limited restraint of potential criminal proceeds when these are detected prior to the formal initiation of a criminal investigation, whether following an STR or consent request by a financial institution, or by supervisory enforcement action, or whether detected from information included in incoming MLA requests from foreign jurisdictions. In all such occurrences, the evaluators have come across examples of unrestrained property, which leave them concerned as to the ability to prevent the flight or dissipation of the assets in such scenarios. These are concerns amplified by the lack of mechanisms for managing complex structures or assets other than funds.

• The robust civil recovery framework introduced in 2009 is not applied in practice by the IoM authorities. Moreover, some of the authorities have limited awareness and do not make use of the legal tools available for civil recovery of property, other than cash.

Recommended Actions

Immediate Outcome 6

• The newly-established FIU should be more proactive in generating intelligence, in accordance with the risk profile of the IoM.

• Actions are underway to progress financial, human and other resources for the FIU and these should continue to be prioritised.

• The capacity of the FIU to collect and analyse information should be increased by, for example, developing an operational analysis handbook.

• FIU staff should continue receiving intensive training in operational and strategic analysis to ensure that the FIU is in a position to perform its functions adequately.

• The authorities should intensify existing measures to improve the SAR regime.

Immediate Outcome 7

• The IoM authorities should establish and apply a clear criminal justice policy on ML investigations and prosecutions setting out the circumstances in which ML investigations need to be initiated reflecting the risk of ML in the IoM especially with regard to the laundering of proceeds of foreign predicate offences.

• Law enforcement authorities should systematically harvest intelligence from all incoming international requests for detection of potential opportunities of effective investigation of ML suspicion regarding IoM based financial institutions and intermediaries.

• Both investigative techniques and the relevant jurisprudence should be further developed to effectively face the challenge of proving foreign predicate offences, even in cases where only limited cooperation from the foreign counterpart is available.

• The IoM should consider further specialisation within its law enforcement, and introduce prosecutorial and judicial resources, and also increase the amount of training for ML. They should consider adding an appointment of a specialized prosecutor and, where possible, support the investigations by the assistance of economic experts or forensic accountants.

• Sanctions imposed so far have not been satisfactory and the evaluation team encourages the IOM to strengthen the sanctioning policy.

Immediate Outcome 8

• Develop a strategy to pursue the effective restraint and confiscation of both instrumentalities and proceeds of crime (and their corresponding value) as a high-level criminal justice policy objective, especially with regard to large amounts of proceeds of crimes committed abroad.

• Develop procedures for systematic initiation of parallel financial investigations aimed at the detection of potential criminal assets subject to confiscation (including restraint of potential criminal proceeds when these are detected prior to the formal initiation of a criminal investigation, e.g. upon foreign request).

• Adopt a more proactive policy for using all available channels through international cooperation in order to initiate restraint or confiscate assets located or moved abroad. The authorities should also take steps to proactively identify foreign proceeds located in the IoM that may be subject to restraint or confiscation.

• Issue guidelines for the application of the proportionality principle both in restraint and confiscation criminal proceedings (including cases of detected undeclared cash) and be more restrained when applying the proportionality principle.

• Systematically apply a civil recovery framework, also in cases where, for any reason, no conviction of predicate offences or ML can be obtained. Additional specialised training on application of the civil recovery framework should be provided to LEAs.

• Introduce a formal and operational mechanism between the relevant authorities: Customs and Excise, the Police, Department of Infrastructure, FIU, IOMFSA, etc. for detecting falsely or undeclared cross-border movements of currency and BNIs. Systematically apply all the available powers to detain falsely or undeclared cash or BNIs in order to determine whether there is a link with ML/FT or associate predicate offences and sufficient grounds for a subsequent forfeiture.

• Determine appropriate mechanisms for managing complex structures or assets other than funds, by appointing a receiver within the criminal proceeding. Consider additionally the possibility of appointing an administrator/controlling accountant at the stage of regulatory investigation.

The relevant Immediate Outcomes considered and assessed in this chapter are IO6-8. The recommendations relevant for the assessment of effectiveness under this section are R.3, R4 & R29-32.

Immediate Outcome 6 (Financial intelligence ML/TF)

196. For much of the evaluation period, the IoM FIU formed part of the IoM's Constabulary's FCU, which also comprised the International Co-operation Unit and the Financial Crime Investigations Unit. There was no clear demarcation between the functions of the FIU and the other units. It was therefore difficult to assess the FIU's performance as a unit separate from the Financial Crime Investigations Unit, which is the law enforcement agency responsible for the investigation of ML/FT. The situation changed in April 2016, days before the date of the on-site visit, with the adoption of the FIU Act, which established the FIU as an independent and autonomous unit situated within the AGC. The FIU has all the powers which are required under the Standards, as indicated under Recommendation 29. The effectiveness of this newly set-up unit could therefore not be measured. The analysis focuses on the situation as it was before the coming into force of the FIU Act.

Use of financial intelligence and other information

(a) Access to information

197. As part of the FCU, the FIU had access to all databases available to other FCU units. This included a wide range of law enforcement, administrative and financial databases held either by domestic or UK authorities[30]. In addition, the FIU had direct access to the CED's database (both in the IoM and in the UK) through the customs officers seconded to the FIU. All the officers of the FIU, being either police or customs officers, had personal communication lines with their counterparts in other law enforcement agencies within the IoM and in the UK. This greatly facilitated access to information.

198. The FIU regularly accesses databases containing law enforcement, administrative and financial information in the course of the analysis procedure. The LEAs met on-site expressed their satisfaction with the information provided by the FIU upon request.

199. During the period under review, the FIU did not have the power to compel the production of additional information from reporting entities. The FIU explained that additional information was provided by reporting entities on a voluntary basis when so requested. The evaluation team could not confirm this as no statistics were made available. Mixed responses were received from the private sector in this regard during interviews. According to the FCU, in practical terms the absence of this power had little effect in the performance of the FIU function, as industry complied with any

[30] The whole list was provided to the evaluation team which was satisfied that it is very comprehensive.

request to provide additional information, especially to improve on the quality of their submitted reports.

(b) Use of intelligence

200. The authorities have presented all the cases (36 in total) where intelligence generated by the FIU following the receipt of a SAR was used by law enforcement authorities to develop evidence related to ML and associated predicate offences. A summary of two such cases is provided below.

Operation Increment

Between March 2010 and November 2010 in excess of 50 SARs were received from banking institutions on the IoM, predominantly from one main high street bank. Cash sums were paid over the counter at branches on the IoM into UK domiciled accounts by third parties living in the IoM. The cash deposits had predominantly been in the region of EUR 235 (GBP200) – EUR 3,525 (GBP 3,000). On each occasion the same amount or a similar amount was withdrawn almost immediately or at most within a 24 hour period in the UK, usually in the Merseyside area. The submitted SARs were disseminated to the FCU investigations team by the FIU function, clearly identifying the potential criminality of money laundering and typology being employed to undertake this crime.

An investigation was commenced named Operation INCREMENT with the overall aim to identify and then prosecute individuals for standalone ML offences. The typology of this type of ML was identified through a number of resources. CCTV showed the individuals entering the bank; the individuals were subsequently identified as persons with previous convictions, usually dishonesty and illicit drug users. Other sources of information were from local knowledge and Police intelligence systems such as the IoM Constabulary's Mentor system, the UK Police National Computer which the Constabulary has full access to and local intelligence databases including liaison with ITD and CED. Intelligence was disseminated to the UK LEAs and additional to the evidence collated on the IoM, it was established that the individuals depositing cash on the IoM had no known link with the UK account holders. It was ascertained the UK account holders in many cases had previous convictions, dishonesty and drug offences. The cash deposits were generally in small denominations of £10 and £20 notes and in Manx currency. The currency withdrawn was always in UK notes.

This typology was disseminated by the FIU function across banking institutions on the IoM. The main bank in question engaged throughout with the investigation unit, having previously been supplied a typology check list which included age, height, clothes worn, accent, gender etc. of the persons paying in. This was supplied by the FCU to help in any future identification and prosecution. This information was to form part of further SAR's that were subsequently submitted by the bank.

As the investigation progressed, further intelligence gleaned was disseminated to LEAs in the UK and IoM. IoM officers travelled to the UK to execute arrest and search warrants on identified individuals receiving criminal funds into their accounts.

As a result of Operation INCREMENT intelligence identified a further 5 individuals undertaking a similar modus operandi. Named Operation Erase the 5 were investigated in the IoM for ML and Drug Trafficking. The 5 individuals involved in depositing cash on the IoM were arrested and prosecuted for ML offences; two of those individuals were also prosecuted for drug trafficking. The highest sentence being 2 years imprisonment for laundering EUR 94, 024 (GBP 80, 000). The lowest being 2 months suspended for 1 year for laundering EUR 2,938 (GBP 2,500). Benefit figures were ordered in excess of EUR 152, 783 (GBP 130, 000) with around EUR 3525 (GBP 3, 000) confiscated.

An intelligence package was sent to UK Police in order for them to deal with the 5 identified account holders. None were prosecuted by the UK authorities. This resulted in an operational decision during the course of Operation Increment for IoM officers to travel to the UK to arrest the account holders and bring them back to the IoM for investigation and subsequently, prosecution. In total, 6 UK account holders were arrested in the UK with the assistance of the UK authorities and successfully prosecuted on the IoM for ML.

As a result of all the aforementioned enquiries and dissemination of the typology to industry this type of offending was effectively stopped in its tracks by the banks refusing to take third party credits. In turn Investigators within the FCU hypothesized that there would likely be an increase in cash being sent through the post. As no legislation was in place to search postal packets for cash at that time, the FIU took the initiative and led in putting forward a proposal to create new legislation which ultimately resulted in the Cash in Postal Packets Act. The Act received Royal Assent on 19 February 2013.

Operation Nickel

The FIU received a SAR from a local financial institution, which divulged that a local resident had deposited a sum of cash for crediting to a third party account held in the UK. The equivalent amount was withdrawn almost immediately from the destination account. Local intelligence checks on the subject of the SAR identified their link to controlled drugs and associated criminality. Further enquiries revealed the subject had deposited a total of around EUR 3,526 (GBP 3000) cash, in multiple tranches ranging from EUR 235 (GBP200)to EUR 1,175 (GBP 1000), in a relatively short period of time, and that these amounts were unlikely to be from legitimate sources as the subject's only known source of income was state benefits. It was suspected the subject was either concerned in drug trafficking or laundering the proceeds of such activity.

Following liaison with the AGC, Production Orders were obtained and served on the financial institution to acquire evidential material, and consequently the subject was arrested for money laundering, and his address searched. Besides other evidential material, EUR 35,264 (GBP 30,000) worth of controlled drugs was recovered during the search. The subject was convicted of 8 money laundering offences, removing criminal property from the IoM, and received a custodial sentence.

201. These cases show that the FIU has successfully assisted LEAs in developing evidence and securing convictions for ML and associated predicate offences. The analysis conducted by the FIU in Operation Increment lead to the identification of a clear typology and third party ML. The case led to the arrest of 19 individual subjects and charges and prosecutions to 16 individuals. In another case, Operation Finder, which was concluded in 2009[31], FIU-generated intelligence assisted LEAs in tracing assets situated in different jurisdictions. Notwithstanding the FIU's successful involvement in these few cases, the FIU's input appears to be limited within the overall system. The FIU's role in most cases appeared to be in assisting LEAs to obtain information. The FIU conducted limited in-depth analysis and, as a result, the intelligence products of the FIU only occasionally added significant value. The analysis process of the FIU mainly consisted in linking incoming SARs with existing ones and seeking information from databases and other domestic and foreign authorities to determine the suspect's economic profile and establish a link to an underlying criminal activity.

202. During the on-site visit, the authorities presented an on-going case involving multiple structures and layering and combined multiple jurisdictions in terms of intelligence gathering, evidence gathering and tracing of assets. The case, the details of which cannot be disclosed as it is still sub judice, demonstrates that the FIU was instrumental in assisting the FCU in handling more complex cases, involving corporate structures with legal entities and arrangements situated in different jurisdictions. However, given the nature of the business conducted in the IoM, the low number of cases of this nature, raises questions about the extent to which intelligence, irrespective of the manner in which it is generated, is effectively used by law enforcement authorities.

203. The FIU was not equipped with IT tools to conduct more advanced operational analysis. The representatives met on-site conceded that the need for such tools had never arisen given that the cases which are dealt with did not often contain any meaningful content. It was, however, pointed out that the FIU employs a dedicated data analyst who is trained to the recognised UK National Intelligence Analyst standard and equipped with software such as Anacapa, i-2 and Altia.

204. No FT Criminal investigations cases were presented to the evaluation team. However, the FIU dealt with a number of FT related SARs which are discussed further within this report.

STRs received and requested by competent authorities

205. The FIU acts as the central authority that receives ML/FT SARs. At the time of the on-site visit, the FIU was in the process of implementing a new electronic reporting system. SARs are predominantly reported by banks. The number of SARs filed by DNFBPs has remained low. The FIU occasionally receives reports from other competent authorities, such as the IOMFSA, the FCU and CED.

[31] And therefore falls outside the period under review.

Table 2: Number of SARs filed by reporting entities

SARs filed by type of business	2008	2009	2010	2011	2012	2013	2014	2015 (1Q)
Accountant	9	14	16	9	17	12	7	5
Banks/Building Society	524	941	949	1162	711	995	811	236
TCSP'	135	207	195	216	196	216	186	46
Financial Advisor	3	0	4	1	2	0	8	3
Investment/Fund Manager	20	24	16	35	22	23	9	8
Lawyer	16	27	41	60	46	37	23	12
Life Assurance/Insurance Company	185	137	166	168	129	125	81	22
Money Service	13	7	5	4	1	0	13	1
Online Gaming	1	6	28	992	97	91	165	80
Other	6	3	5	5	4	6	4	1
Post Office	2	2	5	3	6	14	10	3
Regulator	2	7	4	6	4	8	1	1
Stockbroker	2	7	8	7	9	12	3	2
Total	**918**	**1382**	**1442**	**2668**	**1244**	**1539**	**1321**	**420**

206. There is a real possibility that some FT SARs may not have been reported to the FIU. Some reporting entities met on-site were unclear as to which authority is responsible for receiving FT SARs, while others stated that reporting would not be necessary under current legislation or that FT SARs should be submitted to CED. The authorities were of the view that where such confusion exists, the FIU would be made aware of the disclosure by CED in a very short time. Additionally, it was stated that such an error is unlikely as the only mechanism to report ML or TF suspicions is through the FIU, irrespective of whether or not the reporting entity uses the online function. There is one form proscribed in law that disclosures must be made on, and the reporter has to clearly state the enabling act, POCA for ML and ATCA for TF.

207. The quality of reported SARs is in general perceived as being rather low. The FIU estimates that only around 25-30% of all reported SARs per year actually contain concrete ML/TF suspicions. This holds true for all the sectors. Generally, the authorities met on-site explained that the level of defensive reporting is of concern. This was confirmed during meetings held with the private sector. Many representatives stated that they would report promptly without conducting further internal analysis in order not to risk becoming implicated with a suspicious client.

208. On a positive note, most SARs filed with the FIU appear to be in line with the risk profile of the IoM. They contain indications or solid suspicions on tax-related offences which often involve complex structures established in or outside the IoM. This is evident from the figures in the table below. These SARs are mainly UK-related, and where criminal conduct is suspected, these are reported to the UK Authorities. Another large portion of SARs relate to domestic drug related offences which constitute one of the IoM`s main domestic predicate offences leading to ML investigations and prosecutions. Furthermore, the assessment team has been advised on-site that a large number of SARs are filed by call centres of large multi-national financial institutions situated in the Isle of Man. The FIU estimates that around 300 SARs (app. 20% of SARs on average) are reported by such call centres. However, the vast majority of these do not contain any specific connection to the Isle of Man as these call centres are legally obliged to report on ML/TF suspicions regardless of the origin, involved parties and the nature of the business if the call taker is in the IoM. The FIU raised concerns regarding this practice as it diverts valuable resources that could be used more efficiently.

Table 3: Grounds for suspicion to file an SAR

ALL SARs received:	Year							
Grounds for suspicion	**2009**	**2010**	**2011**	**2012**	**2013**	**2014**	**2015**	**2016 Jan-Mar**
Account Not in Keeping	133	107	154	136	226	189	388	79
Cash Inward/Outward/High Trxns/Forex	161	202	137	89	110	62	121	28
Transaction Support Inadequate	105	64	86	74	97	85	95	26
Court Orders	20	27	21	19	23	0	0	0
Police/Regulator Enquiry	100	107	75	46	56	71	134	25
KYC issues	57	31	30	32	38	39	100	16
Fraud/False Accounting/Forgery	161	130	1118	200	180	188	243	47
Media/Internet Research	151	173	203	199	231	205	264	51
PEPs	13	13	13	12	7	8	10	1
Layering/Complicated Structure	24	19	16	27	29	18	14	7
High Risk Area	47	73	74	36	39	40	34	6
Fiscal	407	484	726	364	496	411	412	121
Corruption/Bribery	3	12	15	10	7	5	6	2
TOTAL	**1382**	**1442**	**2668**	**1244**	**1539**	**1321**	**1821**	**409**

209. The FIU also receives cash declarations above the legally established threshold from CED. Due to the IoM's position as part of a single customs area with the UK, the Common Travel Area for people moving within the British Isles (including Ireland), and the customs territory of the EU, there are no customs barriers between the UK and the IoM. However, the Police and CED carried out regular exercises, targeting both cash and prohibited and restricted (smuggled) goods, such as illegal drugs and tobacco products. In addition, security personnel at the airport and seaport have a function in detecting and reporting unusual cash movements, and have had some success in particular with money being taken from the IoM to the UK for use in suspected drugs purchases.

210. Data provided to the evaluation team shows that in the 6 years to the end of 2014/2015 Customs and Excise received the following numbers of cash declarations –

2010	14	EUR 244,560 (GBP 209,026)
2011	13	EUR 494,540 (GBP 430,035)
2012	12	EUR 775,661 (GBP 630,619)
2013	16	EUR 469,148 (GBP 397,583)
2014	15	EUR 494,418 (GBP 398,924)
2015	12	EUR 474,779 (GBP 344,043)

211. All declarations received are examined and forwarded to the FIU. None have resulted in any ML/FT investigations, since in all cases it was determined that there was a legitimate reason for the transportation of cash. During the NRA CED identified the need for improved cash control at ports and airports. As a first step, it initiated an outreach programme with both private sector and government security personnel at the seaport and airport during 2015. The aim of the outreach was to raise awareness amongst security personnel of the reasons for cash controls, what the requirements were and who to contact. As a result of the interaction with the security staff, in 2015 the Treasury amended the definition of "cash" in the legislation to include stored-value cards and other devices; a potential loophole that the security personnel had raised.

Operational needs supported by FIU analysis and dissemination

(a) Operational analysis

212. The FIU`s input regarding financial analysis is rather limited. The FIU has been successful in assisting LEAs in some cases. However, in most cases the FIU was used to gather additional information for preliminary investigations conducted by the FCU and for ML/TF related incoming MLA requests received by the AGC. Several authorities indicated that the FIU does not regularly deal with multi-jurisdictional, complex cases involving a large volume of transactions that would potentially represent significant proceeds of crime.

213. The FIU receives on average 4 FT SARs per year (6 in 2010, 3 in 2011, 7 in 2012, 5 in 2013, 2 in 2014 and only 3 in 2015). According to the FIU, these SARs were prioritised for immediate action. Of the 26 FT SARs, 12 were renewed submissions on previous subjects. Many of those submissions were simply referring to open source material that had no intelligence value. Analysis of the 26 SARs led to the dissemination of 25 intelligence reports, 6 domestically and 19 internationally. The evaluation team was not informed of the outcome of these disseminations. When examining with the authorities a recent on-going FT SAR analysis regarding an extremely sensitive suspicion of FT involving both the UK and the IoM, the evaluators were surprised to find that the FIU had not conducted any analysis other than disseminating the SAR to the Special Branch of the police. In addition, only a partial and sanitized version of that SAR was forwarded to Special Branch and UK NCA.

214. The IoM applies the consent regime, whereby reporting entities request consent from the FIU to proceed with a transaction after having submitted a SAR. A large number of private sector representatives expressed dissatisfaction with the manner in which the FIU handles most of these requests. Generally, reporting entities are informed that the transaction does not constitute a matter of consent. Industry suggests that this is indicative of the FIU's lack of expertise to draw a definitive conclusion, especially in relation to complex cases. The FIU's view is that industry representatives tend to seek consent even when faced with an unusual transaction or activity which does not fall under the POCA consent regime.

(b) Strategic Analysis

215. The FIU function within the FCU conducted limited strategic analysis in the period under review. The newly set up FIU intends to cover trends, methods and typologies in a more detailed way in its annual activity report. The FIU stated that information on emerging trends, methods and typologies is generally provided in training events for the private sector. However, on-site private sector representatives indicated that more detailed and current information related to strategic analysis should be provided. These views were shared by some LEAs and the IOMFSA. The FIU agreed that further improvement in this area is needed.

(c) Dissemination

216. The FIU disseminates its analysis products to domestic and UK authorities, as indicated in the table below. In past years any SAR received by the FIU with a direct link to a licensed financial entity was passed to the Financial Services Commission ("FSC") (now the IOMFSA). The FSC checked all such SARs against its databases and verified whether they had any regulatory interest. In later years, a more targeted approach has been adopted and only selective SARs are circulated to the IOMFSA. Hence the fall over the years in the number of disseminations to the regulators as shown on the table. The percentage of cases disseminated to IoM LEAs is low when compared to the number of cases disseminated to UK authorities and IoM regulators. This is because local SARs are more likely to be dealt with within the FIU due to local knowledge on such a small island and on average, only about 10% of SARs received relate to IoM individuals and entities.

217. The FIU explained that higher end cases are disseminated to the Joint Tasking Group, which is chaired by the IoM Constabulary and comprises representatives from the FIU, the FCU, the Crime

Support Team of the IoMC, the AGC, the ITD and CED. The Joint Tasking Group is a forum for partners to work collectively to address serious crime, particularly ML and FT. Not many cases have been dealt with by the Joint Tasking Team in the period under review. Other cases are dealt with directly by the FCU. Each case is assessed against a threat, risk and harm matrix. On a day to day operational basis, the FCU reviews caseload every two weeks and where necessary makes adjustments so as to ensure that priority cases are resourced adequately.

218. Table 4 indicates the number of intelligence reports related to SARs disseminated by the FIU.

	2008	2009	2010	2011	2012	2013	2014	2015
IoM LEAs	65	103	173	100	65	115	71	106
IoM REGULATORS[32]	503	680	375	234	229	114	59	57
IoM Other	0	0	0	4	1	1	0	1
Domestic Total	568	783	548	338	295	230	130	164
UK FIU	491	504	288	256	145	213	163	139
UK LEA	171	278	129	154	128	115	70	45
SCHEDULE A[33]	198	303	239	253	152	231	174	221
Total	1428	1704	1204	1001	720	789	537	733

219. Table 5 below contains the actual number of cases disseminated to LEAs in the IoM. The authorities were not in a position to indicate the number of investigations which were initiated on the bases of these disseminations. They pointed out that due to the recording systems in place it was not possible to extrapolate the number of SARs disseminated to IoM LEA's without physically researching each individual case across a number of data platforms. Dissemination to other jurisdictions was also not readily captured[34]. The FCU undertook a physical case-by-case examination of SARs submitted during 2015 to provide a better understanding of how many SARs resulted in actual investigations. Of the 67 that were disseminated to the Constabulary in 2015, 8 resulted in further investigations by the FCU that year and were linked by nature of nominals and associates. A further two SARs submitted in this period also supported on-going financial and money laundering investigations. The majority did not result in prosecution but further investigations were undertaken to investigate the SARs.

Table 5: Number of disseminations sent to LEAs and others for investigation or other action

LOCAL DISSEMINATIONS	2009	2010	2011	2012	2013	2014	2015
IoM Police/FIB	83	125	57	26	64	46	67
ITD	16	32	32	26	34	20	23
IOM C&E	4	13	11	11	16	3	12
DHSC	0	2	0	0	1	1	3
FSA[35]	679	370	226	216	97	53	55
IPA	1	5	6	5	3	3	0
GSC	0	0	2	8	14	3	2
Work Permits	0	0	1	0	0	0	0
IMMIGRATION	0	1	0	2	0	0	0

[32] The high figures reflect the approach taken by the FIU at the time which was to forward the majority of SARs to the FSA for review.

[33] Schedule A FIUs are; Argentina, Uruguay, Brazil, Denmark, Eire, USA, Netherlands, France, Guernsey, Jersey, Mauritius, South Africa, Spain, St Vincent, Cyprus.

[34] This is an objective captured within the NRA and future strategic plan for the FIU in its collation of feedback vs. SARs and intelligence disseminations

[35] These figures include all disseminations sent to the FSA and it is not possible to extract the figures relating to cases for further investigation or other action

LAW SOCIETY	0	0	0	1	0	0	0
OFT	0	0	0	0	0	1	1
Aircraft Agency	0	0	0	0	1	0	1
E-Commerce	0	0	1	0	0	0	0
Attorney General's	0	0	2	0	0	0	0
TOTAL	**783**	**548**	**338**	**295**	**230**	**130**	**164**

220. Disseminations by the FIU to the IOMFSA have been used successfully to take regulatory action. For instance, in Operation 'Storm', which related to a high level Merchant Card service provider that was defrauded, the FIU-disseminated intelligence and investigation updates led to regulatory action under the Company Officers (Disqualifications) Act (CODA) of 2009 to remove the individual concerned as a director. In Operation 'Cobalt', relating to theft within a FI, intelligence shared with the IOMFSA led to further regulatory investigation of the company as a whole for poor record keeping and not having adequate preventative measures in place. In another case, the FIU disseminated intelligence to the IOMFSA regarding an attempt to fraudulently obtain IoM Government funding for a start-up company through a local CSP. Action as a result of the intelligence dissemination and further investigation by the IOMFSA resulted in the CSP having their licence revoked.

Cooperation and exchange of information/financial intelligence

221. The FIU regularly exchanged information with the other units within the FCU. The IOMFSA and FIU have long had a close working relationship on both an officer level and an operational level, including reporting to the IOMFSA where unusual volumes of SARs are identified or where poor quality SAR reporting has been identified. Information passes in both directions between CED and the FIU, aided by the presence in the FIU of a number of customs officers deployed there. The GSC advised that while there were discussions from time to time with the FCU/FIU on specific issues (for example, SAR quality from the gambling sector, discussions on typologies, etc.) there was no systematic gateway for passing intelligence from the FCU/FIU to the GSC. It was noted that the GSC systematically passes beneficial ownership information to the FCU.

222. On a national level, the FIU is represented in the AML/CFT Strategic Group which, as stated in Chapter 1, comprises various government authorities, including high-level political stakeholders. Under the previous regime, the FIU was represented in the AML/CFT Strategic Group by FCU staff members.

223. With respect to confidentiality of information, it was noted that all FIU information is registered in the Government/Police secure computer server and can only be accessed by authorised personnel. This is in accordance with procedures laid out in the Isle of Man Government Corporate Information and Records Management Policy. Dissemination of information is covered by legislation (POCA 2008 sections 210-214, ATCA 2003 sections 56–57, and the DPA 2002), together with internal FIU policies and procedures. Police Officers employed within the FIU are also covered by Police Disciplinary Regulations covering the improper disclosure of information. Customs officers and civil servants attached to the FIU are required to comply with IoM Civil Service Regulations for disciplinary matters and the Official Secrets Act protecting the confidentiality of the information. FIU-specific information, such as SARs and information from foreign FIUs, is also stored on the police computer. Access is restricted to the FIU analysts and supervisors. It is shielded from direct access by other investigators by 'interest markers', so any information release has to be cleared by the head of the FIU.

Conclusion

224. **The IoM has achieved a low level of effectiveness for Immediate Outcome 6.**

Immediate Outcome 7 (ML investigation and prosecution)

ML identification and investigation

225. The Financial Crime Investigation Unit within the FCU is the investigative unit responsible for the investigation of money laundering. The number of ML investigations conducted by the FCU, indicated in the table below, remains rather low.

Table 6: Number of ML Investigations with or without an STR						
Year	Investigations leading to Prosecutions		Investigations NOT leading to Prosecutions		ML investigations whether leading to a Prosecution or not	
	Cases	Persons	Cases	Persons	Cases	Persons
2010	5	26	1	1	6	27
2011	9	10	2	3	11	13
2012	5	6	2	12	7	8
2013	6	7	10	12	16	19
2014	2	2	9	11	11	13
2015	1	1	10	15	20[36]	36

226. The FCU rarely conducts complex financial investigations to address the ML risks that the IoM faces. In those cases where this was a necessity, there was support from the Senior Command Team and DHA to ensure adequate expertise and support was funded beyond the general work of the investigators. This catered for expertise such as complex financial accounting and tracing the movement of funds. In discussions with the IoM authorities, the evaluators were encouraged to hear of the recruitment of experienced retired financial investigators which has primarily been funded by the seized assets fund. They have supported criminal investigations over the last 2 years.

227. The CED and the ITD are authorised to conduct investigations regarding predicate offences which fall under their activity, mostly being money laundering associated to drug-related offences (CED) and tax offences (ITD). The ITD has not conducted any ML investigations. An investigation undertaken by CED involving customs, excise or VAT fraud inevitably involves tracing funds used or obtained in the fraud. According to the CED, the investigating officers undertake both the fraud and ML investigation, at least in the early stages. In cases involving any significant suspected ML, it would be referred to the Joint Tasking Group for a decision on the best and most appropriate use of resources. According to the authorities, the FCU is seen as the lead agency in such investigations, with the CED providing assistance and resources (as well as continuing any parallel investigation involving the predicate offence, if necessary). It would appear that the CED has not conducted any ML investigations itself.

228. Due to the size of the IoM, there seems to be no impediment as to the timeliness in which competent authorities can potentially obtain or access relevant financial intelligence and other information required for their ML investigations. Joint and co-operative investigations between different competent authorities such as the FCU and the CED, in full coordination with the IOMFSA, are all possible and have occurred though not as commonly as expected. In these investigations several available investigative techniques have been used, although the evaluators have been informed that not all have been applied in ML investigations. During the on-site assessment, the FCU shared evidence of the department's Terms of Reference which supports the above approach and the training pathway. This pathway has been driven by the FCU Strategic Board and was one of the objectives on the strategic plan, also identified as part of the IoM's NRA.

229. The FCU is engaged mainly on domestic predicate crime that generates the highest proportion of domestic proceeds albeit not significant proceeds. The FCU does not appear to take a more

[36] 2015 figures include 9 on-going cases under investigation and 20 individuals.

proactive approach to identify, initiate and prioritise complex ML cases, involving potential abuse of or by the IoM financial sector where property is the proceeds of foreign predicates. The FCU lacks a full time forensic accountant who would assist in focusing the deployment of resources and the analysis of complex material[37]. The authorities are of the view that when such cases present themselves, there is the necessary expertise which can be called upon, as demonstrated in the 2009[38] Baines case, where the suspect was convicted of laundering US $175 million deriving from a securities fraud in the United States. The investigation in that case was initiated as a result of an SAR filed by a bank in the IoM. The evaluation team remains of the view that the FCU has been rather reactive in this area.

230. During the on-site visit, the attention of the evaluators was drawn to cases where suspicion of ML relating to the activity of TCSPs had arisen, e.g. as a result of supervisory action or reporting of SARs. After discussing these cases with the authorities, it emerged that potential cases of ML have not been promptly and appropriately identified and investigated. The fact that potential ML cases have gone undetected for a long time calls into question the proactivity of the authorities in identifying and investigating ML cases.

231. The FCU does not conduct parallel financial investigations on a regular and systematic basis with respect to major proceeds-generating crimes. The authorities make the point that SARs play a very effective part in the detection of ML whilst acknowledging that most cases have been initiated without one. Only 36 investigations have been initiated based on a SAR in the period under review. There appears to be an under-utilisation of SARs. The ratio of intelligence disseminated to the FCU to indictments from 2010 to 2015 is 7.3% (28/385).

232. A potential reason for this may be the low quality of SARs. The evaluators came across several cases where reporting entities did not submit a SAR despite the existence of the conditions to do so. Other examples raising some concern were cases where potential suspicion was discussed by the banks with TCSPs, which had introduced clients to the banks, prior to SAR reporting, where the bank might have had suspicions concerning the TCSP itself.

233. Another aspect typically missing in the investigation process of ML is the international component. The IoM competent authorities only rarely seek international co-operation. This is surprising considering the nature of the IoM as an international financial centre and the involvement of foreign corporations in the typical structures formed in the IoM. Additionally, no domestic ML investigations have been initiated as a result of an incoming MLA request regarding ML or predicate offences committed abroad. The assessors remain therefore concerned as to the low extent to which law enforcement agencies are seeking appropriate assistance from their foreign counterparts in cross-border ML cases.

234. The evidence obtained from incoming MLA requests has not been examined to determine whether any relevant intelligence may be harvested. At the time of the on-site visit a project was underway to find ways how this can be effectively undertaken. The intention is that all future evidence will be scanned and saved in digital format so it can be searched for intelligence or any indication that an institution or person has been assisting in ML.

235. The AGC is in charge of reviewing the cases, advising on charges and where appropriate preparing indictments and prosecuting ML offenders. The AGC may be considered to be under resourced to deal with the potential increase in workload and the addition of large, complex ML cases which may involve months of litigation. The Prosecution and the Defence are entitled to apply on a case by case basis for a case specific temporary advocate's licence enabling a non-Manx advocate to appear as an advocate in Court in a particular case. This is a useful facility which can enable flexibility in resourcing although reliance cannot be placed upon the granting of a temporary

[37] The evaluators acknowledge that even with such a permanent resource some outsourcing of forensic accounting would be necessary.

[38] Outside the period under review.

advocate's licence, which may be opposed or not granted, which has been the situation in recent times.

236. When discussing the reasons for not properly investigating several cases of suspicion of ML, it was apparent that the FCU and the AGC do not always interact with each other in an effective enough way throughout the life-cycle of a ML case. The evaluators accept that in a common law jurisdiction such as the IoM it is the police which has the task of investigating a criminal case and not the prosecution. Nevertheless, it seemed that there was mutual agreement as to the need for greater prosecutorial involvement at the earlier stages of the financial investigation. This was not possible due to the heavy workload of the prosecutors. To-date there has not been a prosecutor with the specialised task of leading more complex financial investigations. However, the FCU demonstrated the use of independent expert counsel within one on-going complex ML case.

237. The evaluation team noted some instances where supervisory enforcement measures were pursued in lieu of a ML investigation. These measures are in themselves welcome and serve an important preventative goal. Nevertheless, they create an over-reliance by FCU on the "non-criminal" enforcement actions taken by IOMFSA. This hampers the effectiveness of both potential successful investigations of ML and the confiscation of assets which are, as a result, not restrained. This is caused especially because of the significant delay until such regulatory action is concluded. The reliance by the FCU on action being taken by the regulator is an indication of its limited capacity to investigate such suspicions. If criminal action were to be taken, this would ultimately have a more significant impact on the deterrence factor.

Consistency of ML investigations and prosecutions with threats and risk profile, and national AML policies

238. The types of ML activity being investigated and prosecuted in the IoM are not consistent with the country's threats, risk profile, and national AML/CFT policies. The identified risk in the IoM is that intermediaries may be used for layering the proceeds of crime where the predicate offence has occurred outside the IoM. In the period under review, no prosecutions were initiated in cases involving reporting entities, especially TCSPs and other professional intermediaries (failure to report, concealment or being involved in an arrangement). Until recently, there have been no domestically initiated ML cases involving foreign predicate offences (tax, fraud, corruption etc.) and no conviction of ML regarding a foreign predicate offence. So far, there has only been one such case in 2009 (Baines). The evaluators were informed of one on-going investigation which allegedly involves a foreign predicate offence of significant scale. All ML prosecutions and convictions over the period under review relate to domestic predicate offending.

Types of ML cases pursued

239. The prosecution has demonstrated an effective ability of prosecuting a wide variety of ML cases (though as described above not commensurate with its risk assessment). As can be seen in Table 8 below, almost 42% of the convictions for ML (25 of 59) were third-party ML cases; 12% of the convictions for ML (7 out of 59) were stand-alone (or autonomous ML cases) as opposed to self-laundering (see e.g. Operation Increment described under IO6). There is no impediment to achieving convictions in stand-alone ML cases. Case practice proves that the absence of a conviction for a predicate offence is not an obstacle to a conviction for ML, though such cases have significantly reduced in recent years.

240. In the period under review, the predominant acquisitive domestic predicate offending was drug related. Third party ML and autonomous ML cases have succeeded despite the absence of a conviction for a predicate offence, as a result of inferences drawn from the defendant's conduct and the surrounding incriminating circumstances. The courts are willing to accept inferences drawn

from facts and circumstances to establish elements of the ML offences, following non-binding but persuasive English jurisprudence in this area.

241. To date, only natural persons have been prosecuted and convicted for ML.

242. The most significant criminal cases are tried by jury before the Court of General Gaol Delivery presided over by a judge, known as a Deemster. Appeals from that court are to the Appeal Court, known as Staff of Government. Appeals from Staff of Government are to the Judicial Committee of the Privy Council which is the highest court of appeal for the Crown Dependencies. The First Deemster, who deals with civil rather than criminal cases, also sits with the Judge of Appeal (who is an English Q.C.) in Staff of Government. The First Deemster also appoints Panel Deemsters. Panel Deemsters are Q.C.s from England and Wales who have sat periodically as Judges ('Recorders') over many years in England and Wales. Panel Deemsters may have a criminal or civil law area of expertise. Those who sit in fraud and ML cases have many years' experience as barristers and as judges in conducting fraud and ML cases in England and Wales. This specialised experience could not be readily obtained by practising exclusively on the IoM because of the relatively small number of cases proceeding through the courts. A Deemster who tries a jury trial case may either be the one permanent Deemster who deals with criminal cases or a Panel Deemster appointed by the First Deemster and selected from the panel on a case by case basis. When the court administration selects a particular Deemster to sit in a fraud or ML case it is particularly valuable to draw upon the resource of greater experience of the panel Deemsters in appearing in and acting as Judges in such specialised cases. The Deemsters of the IoM have excellent reputation and are independent.

Table 7

	Prosecutions commenced			Convictions (first instance)			Convictions (final)		
	Cases	Natural persons	Legal persons	Cases	Natural persons	Legal persons	Cases	Natural persons	Legal persons
2010	6	11	0	5	9	0	5	9	0
2011	4	5	0	4	5	0	4	5	0
2012	10	11	0	9	10	0	9	10	0
2013	4	4	0	3	3	0	3	3	0
2014	3	4	0	1	1	0	1	1	0
2015	4	5	0	4	5	0	4	5	0

Table 8: Different types of convictions

	Total	Self-laundering	Number of convictions for third party laundering	Number of convictions for stand-alone (or autonomous ML	Number of convictions for laundering proceeds of crime committed abroad	Number of convictions for fiscal predicate offences	Number of convictions for non-fiscal predicate offences
2010	14	7	5	2	0	0	14
2011	20	6	13	1	0	0	20
2012	15	8	6	1	0	0	15
2013	3	1	0	2	0	0	3
2014	2	2	0	0	0	0	2
2015	5	3	1	1	0	0	5

Effectiveness, proportionality and dissuasiveness of sanctions

243. Sanctions applied against natural persons convicted of ML offences are only partially effective and serious doubts remain as to their dissuasiveness. The evaluators remain uncertain as to the

extent to which the protected value of the crime of ML is understood in the IoM and as a result the indictment of ML is not always pursued.

244. The following table is intended to provide an indication of the effectiveness of the criminal sanctioning regime and should give an indication of the severity of the penalties imposed for ML offences. The IoM authorities pointed out that in every case between 2010 and 2015 (save for three) the convictions had resulted in a custodial sentence (usually immediate but sometimes suspended). Nevertheless, the sentence was, in many cases, an overall sentence which also covered other offences. Self-launderers typically receive sentences which are concurrent to the sentences for their predicate offending and conviction of ML does not usually add much if at all to the sentence. They additionally referred to the growing number of guilty pleas which they see as an indication that the defendants themselves recognise the capacity of juries to draw irresistible inferences. While this is true these guilty pleas could also reflect a lack of dissuasiveness.

245. The evaluators were especially concerned in this context with the outcome of the case involving an advocate and convicted of laundering the proceeds of crime – a conviction that was subsequently quashed by the Privy Council (Holt v Attorney General [2014] UKPC 4). The evaluators were somewhat surprised that following the conviction of such a serious crime related to such a landmark case (Baines), the advocate had only received a suspended sentence of 12 months imprisonment, which may indicate as explained above that sanctions applied against persons convicted of ML offences cannot be considered dissuasive.

Table 9

Year	Non-custodial sentences			Custodial sentences			
	Fines (average in EUR)	Other than fines	Total number	Imposed prison sentence (average in months)	Suspended prison sentence (average in months)	Other measures	Total number
2010	None	None	None	11.75	3.3	None	15
2011	None	None	None	6.91	7	None	21
2012	None	None	None	6.2	3.25	None	14
2013	391 Euro	None	2	12	None	None	1
2014	None	None	None	4.5	3	None	2
2015	None	None	None	8.33	7	None	4

Alternative Criminal Justice Measures

246. The IoM has not properly applied other criminal justice measures in cases where a ML investigation has been pursued but where it was not possible, for justifiable reasons, to secure a ML conviction. According to information provided by the IoM authorities on site, non-conviction based civil recovery, though available in legislation, is used only with regard to cash seizures.

247. In discussions with the authorities the evaluators were surprised to find that the FCU did not use these measures. The authorities are strongly encouraged to make use of these in appropriate circumstances when a criminal conviction cannot be secured.

Conclusion

248. **The IoM has achieved a low level of effectiveness for Immediate Outcome 7.**

Immediate Outcome 8 (Confiscation)

Confiscation of proceeds, instrumentalities and property of equivalent value as a policy objective

249. The IoM legal framework on restraint and confiscation is comprehensive. It provides adequate tools for detection, restraint and confiscation of instrumentalities and proceeds of crime, both for domestic and international criminal cases. It also provides for a sound non-conviction based civil recovery regime.

250. Notwithstanding that, confiscation of proceeds, instrumentalities and property of equivalent value is not pursued as a policy objective. In those cases where confiscation is considered by the law enforcement agencies, the legal principle of proportionality may have been over-relied on by the prosecution authority. In some cases this has led to situations where not all possible assets have been confiscated. The limited cases that exist suggest that the court has, following consideration of the evidence placed before it and being otherwise satisfied that it is appropriate for it to do so, granted the application for a confiscation order.

251. The focus remains on the restraint and confiscation of proceeds from predicate crime (e.g. drugs, theft offences). However, though the predominant acquisitive domestic predicate offending is drug related, the majority of cases involve small amounts of proceeds and do not facilitate the analysis of the system's effectiveness.

252. Looking at the unpersuasive figures regarding confiscation, especially when compared both to GDP and the volume of assets held in the IoM, it can be concluded that though pursued occasionally, confiscation is not pursued as a high priority policy objective. The overall value of property restrained and confiscated remains extremely low and does not reflect the risks in the IoM.

253. Parallel financial investigations aimed at the detection of potential criminal assets, subject to confiscation, are not systematically applied, especially not in cases where the associated predicate offences occur outside the country. In respect of the latter, the Action Plan developed as a result of the NRA establishes as an objective actively seeking opportunities for parallel or joint investigations with law enforcement agencies in other jurisdictions, where an IoM connection is identified. No specific results were reported in relation to this target. Consequently, it remains part of the policy framework with no substantiated outcome.

254. The NRA identified the actions in respect of financial crime investigations as a top priority, and the Action Plan emphasises that a sustainable training programme for officers involved is required. The information provided by the authorities, although very limited, with regard to the implementation of this objective in response to the Action Plan indicates that the training programme for officers is in place and is managed by the Constabulary. Nevertheless, to date, as can be seen from some ML cases that resulted with a conviction, no confiscation seemed to have been requested, and consequently applied. In those cases, where a financial investigation was conducted in relation to predicate crimes, no sufficient consideration was given to pursue a ML conviction which could have led to confiscation of other assets subject to confiscation.

255. Additional concerns remain over the limited application of restraint of potential proceeds, when these are detected at the earliest possible stage of a criminal investigation, whether detected following a SAR; a consent request by a financial institution; supervisory enforcement actions; or on the basis information included in incoming MLA requests. In all such occurrences, the evaluators have come across examples of unrestrained property which gives rise to concerns as to the effective prevention of the flight or dissipation of the assets.

256. Restraint and confiscation is provided reactively upon request of foreign jurisdictions. On the other hand, the authorities do not make sufficient use of their powers to make appropriate inquiries

from foreign jurisdictions in an attempt to identify, repatriate, share or return proceeds and instrumentalities of crime.

257. The concerns of the assessors with regard to the effectiveness of the confiscation regime are even more relevant in the context of the range of available criminal and civil proceedings tools which are at the disposal of the IoM authorities. For example, although a sound civil recovery regime exists in the legislation, it is not used in practice. There is only one case when the authorities executed a recovery order at the request of a foreign authority and, since 2010, no other application for civil recovery has been made.

258. There seems to be a lack of an overarching policy between the Police and the CED for the detection of falsely or undeclared cross-border movements of currency and bearer negotiable instruments, which results in a lack of policy regarding confiscation of these, if detected. In the rare cases when such cash was detected, no confiscation or seizure has been applied.

259. Both the existing mechanism and the practice in relation to asset management also substantiate the conclusion that confiscation is not being pursued as a policy objective. The powers for appointing a receiver are regularly applied in civil litigations and are not being used by the law enforcement authorities in criminal cases.

Confiscations of proceeds from foreign and domestic predicates, and proceeds located abroad

260. In the last 6 years there were no substantial ML cases and consequently no significant proceeds of ML have been restrained or confiscated. However, there has been one significant confiscation order in relation to a predicate offence. Due to the lack of pro-activeness with regard to ML investigations (as described under IO7, to date only natural persons have been prosecuted and convicted for ML), especially cases involving TCSPs, there has been no confiscation of assets held by intermediaries or corporate structures.

261. The authorities have provided statistics to illustrate the effectiveness of the restraint and confiscation measures, yet most of the cases related to drug offences. As can be observed from the figures included in the Table 10 below, there is a slight improvement in terms of the amount of confiscated property during the last two years. Nevertheless, compared to both GDP and the volume of assets held in the IoM, the overall value of the property restrained and confiscated remains extremely low, and does not reflect the risks of the IoM.

Table 10: Property seized and confiscated

Year	Property restrained/seized		Property confiscated	
	Cases	Amount (EUR)	Cases	Amount (EUR)
2010	9	36,172.68	11	46,949.24
2011	2	4,072.89	12	4559.72
2012	0	0	15	58,873.24
2013	1	11,333.36	4	29,141.3
2014	14	88,830.05	6	1,497,551.08
2015	8	46,330	5	265,678.5

262. One of the reasons for the low number of confiscation orders appears to stem from the application of the proportionality principle. Under the proportionality principle, the investigator will only investigate and seek to restrain (and the prosecutor will only make an application for a confiscation order with respect to) property that is believed to be proportionate in the circumstances of the case. On-site, the authorities referred to some examples where restraint or confiscation of property belonging to or in the possession of the suspect or accused would be deemed disproportionate, even when a legal basis for restraint and confiscation may exist and where

there were indications that the suspect or accused may be leading a lifestyle beyond his means. For instance, in some cases it was considered disproportionate to seek a confiscation order for property other than that which was equivalent to the damage caused to the victim. In other cases, no confiscation was sought beyond the value of the benefit obtained by the offender, even where additional property equivalent to the laundered money or instrumentalities could have been sought. In yet another example, the authorities only restrained the property requested by a foreign authority, without considering whether other available assets could have been subject to confiscation. In this particular case, the lack of proactive approach might have had a negative impact on the real estate market in the IoM. It is to be noted that this rigid interpretation at the investigatory stage is to some extent in contrast with the wide range of possibilities available under the current legal framework, enabling the scope of the confiscation to be defined by the lifestyle of the criminal. The LEAs and AGC seemed to suggest that unless they adhered strictly to the proportionality principle, the court would not authorise the confiscation order. However, the evaluation team noted that, in all cases where the prosecution brought forward a request for confiscation orders, the court has invariably, following consideration of the evidence placed before it and being otherwise satisfied that it is appropriate for it to do so, granted the request. This indicates that the courts tend to consider confiscation orders favourably. Thus, in the opinion of the evaluators, the investigators and prosecutors should adopt a more far-reaching approach when restraining assets and bringing forward requests for confiscation, as it is likely that these requests will not be turned down by the courts, as long as they are supported by sufficient evidence.

263. In addition to the principle of proportionality, other legal mechanisms are in place to ensure the fairness of the confiscation regime (i.e." living expenses"). A restraint order may be made to the extent that assets are available to the accused for reasonable living and legal expenses or for the purpose of enabling the person to carry on any trade, business, profession or occupation. While this is of course acceptable, the implementation of this principle may potentially hamper the effectiveness as there is no fixed or universally permitted amount. This will depend upon the circumstances of the case, and those of the alleged offender. Nevertheless, the actual value of the confiscated assets may end up much less than the amount originally restrained. Though the authorities indicated that there were no domestic cases where large sums have been permitted for expenses from the restrained funds, one case involving a foreign request for confiscation illustrates that, due to the lengthy duration of the legal proceedings in another jurisdiction, the value difference between the original restraint order, the actual enforcement of the confiscation order, and amount of the released sums can be significant (for instance, about EUR 20,818 were realised from the restrained account which held EUR 89,083, within a period of two years and seven months).

264. Another potential area of concern with regard to the effective application of the current confiscation regime is in cases were a compensation order has been additionally granted. Though it is possible to apply confiscation and compensation orders, the predominant practice appears to be limited to requesting only compensation orders under the Criminal Law Act ("CLA") of 1981, which is the payment for any personal injury, loss or damage resulting from the offence. As a result, the confiscation of instrumentalities, laundered property or any profit from the proceeds, is not considered or pursued in such cases.

265. As it can be seen from several ML cases that resulted in a conviction, no confiscation seemed to have been requested (See Thomson, Stephen Gilmore, etc.).

266. Where efforts are put into confiscating the proceeds of crime, in addition to the penalty and the fine for an offence, insufficient consideration is given to pursing a ML conviction and, subsequently, to assess the possibility of confiscating other assets subject to confiscation, such as instrumentalities, for example (e.g. Le Moignan case). This applies particularly to offences committed by individuals acting alone. In such cases, there is often no separate money laundering charge, as it is considered that it would not add to the penalty for the main offence.

267. Over the 6-year period, the predominant acquisitive domestic predicate offending was drug related (42 out of 51 convictions were drug-related, that is - 82%). The IoM authorities indicated that the majority involved small amounts of proceeds and were not high profile cases. In these circumstances, it is difficult to assess the effectiveness of the system based on the analysis of relatively small cases associated with predominantly local drug offences. Another relevant aspect is the ratio between the benefit from the criminal conduct and the actual confiscated amount. Even in some examples of small cases involving self-laundering from drug-related offences, where the benefit varied between £9,000 and £49,320, the confiscation orders were made in the nominal amount of £1, due to the absence of any available property. Nevertheless, some presented cases demonstrate that, after the conviction, the confiscation order can be varied to include an increase up to the benefit from the criminal conduct, when the authorities identify any available property (coming from inheritance, pension, etc.).

268. POCA provides a strong basis for a non-conviction based confiscation regime. The powers in relation to civil recovery and cash seizures can be applied to any property, including cash, whether or not any proceedings have been brought for an offence in connection with the property. Notwithstanding that, these powers are underused. Moreover, the Police appeared not to be even aware of the possibility of civil recovery of property, other than cash seizures. This could serve as an explanation, to some extent, as to why, to date, there is only one case (since the legal basis entered into force (2009)) where the AGC made an application for civil recovery. In respect of the latter, the application made in 2010 was triggered by a foreign civil recovery order received from the UK with regard to funds related allegedly to drug trafficking.

269. No formal arrangements for asset sharing are in place. In this respect, the authorities indicated that there are discussions with the USA in relation to an asset-sharing agreement. The IoM is dealing with asset repatriation and sharing on a case by case basis. Consequently, the principle of sharing depends on the circumstances of the particular case, including any variations to the restraining order as a result of the consent to provide living expenses. The authorities indicated that a proportion of 60% is usually shared. In the case of the UK civil recovery order mentioned above, it was agreed that 80% of the property recovered would be paid to the UK authorities, while 20% would remain in the IoM.

270. The IoM has seized and confiscated proceeds of crime upon request of foreign jurisdictions (as described under IO 2). In recent years, the IoM has in several cases acted upon the requests of foreign jurisdictions for the restraint of suspected criminal assets.

271. Nevertheless, the lack of pro-activeness in international cooperation can be observed. There have been, so far, no cases where the IoM initiated seizure or confiscation of assets which were in or had been moved to other countries. This is especially relevant to the IoM, being an international financial centre. In discussions both with the financial institutions and other authorities in the IoM, it was evident that many structures formed on the IoM, especially in cases in which suspicion has been raised as to the source of wealth, involved foreign companies and foreign natural persons.

272. No effective measures are in place to ensure that the restrained and confiscated property are preserved and managed adequately. The appointment of a receiver to manage complex structure or assets other than funds has never been made, despite the possibility existing in law. Although regularly applied in civil litigation, the powers are not being used by the law enforcement authorities. As indicated by the authorities, the practice is that the goods, other than cash, are left under the responsibility of the offender. No other framework is in place for managing and overseeing the management of frozen, restrained and confiscated property and the current powers are not applied in criminal or civil recovery proceedings. All confiscated money and the funds deriving from the sale of confiscated property are placed into the Seized Assets Fund, managed by the Treasury. Nevertheless, the evaluators were informed that the funds placed into the Fund derive mainly from the confiscated cash and bank accounts.

Confiscation of falsely or undeclared cross-border transaction of currency/BNI

273. There are no customs barriers between the IoM and its surrounding neighbours or any fixed border controls to oversee the movement of people. This is a consequence of the IoM's constitutional nature, 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 IoM and the UK under the Customs and Excise Agreement 1979. The Isle of Man is also part of the customs territory of the EU under Protocol 3 to the UK Act of Accession, which allows for a free movement of passengers and freight between the UK and the Isle of Man.

274. In practical terms, there is no permanent customs presence at sea ports or the airport and there is no requirement for persons entering or leaving the Isle of Man to make any declaration or present themselves to customs or immigration officials, except in specific circumstances (e.g. when passengers arrive directly from outside the CTA or when persons are carrying cash amounting to over €10,000).

275. According to the NRA, the main potential sources of threat are illicit cash, criminal property and drugs. Nevertheless, the focus appears to be on the detection of prohibited/restricted items, such as drugs, rather than the illegally smuggled or falsely declared/ undeclared cash though that does not indicate that risks involving cash movements are completely ignored. The law also allows the examination of UK mail (which is regarded as "domestic" to the customs union with the UK) in respect of situations where it is suspected that a postal packet contains cash. During 2016, for example, an outgoing postal packet addressed to the UK was detained at the Sea Terminal, opened and found to contain a sum of cash liable to detention (below the €10,000 declaration threshold, but suspected of being linked to the purchase of illegal drugs). During 2015, the CED carried out 16 operations at the Sea Terminal in conjunction with the police canine unit using drugs and cash detection dogs. It also carried out 8 visits to freight haulier/courier premises, again with the police canine unit. The canine unit also carries out regular checks on domestic (UK) mail with the co-operation of the Post Office.

276. Outreach activities have been provided to the security personnel (private sector and government employees) who are most likely to come upon illicit cash. The staff were provided with pocket-sized cards summarising the requirements, the definition of what is regarded as being "cash", and what to do if any suspect cash were found. As a direct result of the outreach, and following a suggestion from the private sector airport personnel, the Treasury amended the definition of "cash" in the legislation to widen it, particularly to include "stored-value cards" which had been identified as a potential risk.

277. The NRA concludes that the national ML/FT combatting vulnerability is medium to low with respect to the quality of border controls and low with respect to the effectiveness of controls by the CED on cash and similar instruments. The NRA does not consider the threat of cash entering into the IoM to be high. It is stated that there is evidence to support the view that it has become much more difficult in recent years to place illicit cash directly into banks or other institutions. However, in the absence of information on cash movements, it is unclear how the authorities could have reached such a conclusion. It should also be noted that the UK's NRA identifies cash-couriering as a high risk, which could also have an impact on the risk faced by the IoM, since there are no borders and cash may be freely transported into the IoM. The UK NRA post-dated that of the IoM and was therefore not addressed. The NRA only states that the UK does not regard the IoM as a significant cash courier risk.

278. In this respect, the UK's NRA evaluates the ML/FT risk associated with cash couriering as high. Likewise, although passengers need to declare movements of cash over €10,000, there is no enforcement of disclosure requirements and no random searches conducted on a routine basis. This leads to lack of complete or accurate data which would provide the full picture.

279. Initially, the authorities presented the following figures (see Table 11 below) which indicate that no suspicious incidents occurred during the last 6 years. Nevertheless, the NRA makes reference to a number of cash seizures made as a result of co-operation between the Department of Infrastructure and IoM Constabulary, during the period 2013-2015, at the ferry port (14 stops involving cash detentions) and at the airport (4 cases). Subsequently, the assessors were presented with statistics on cash seizures and forfeitures, however it is not clear how many of them are linked to suspicious cross border incidents, as none are reported.

Table 11: Cross border transportation of currency and bearer negotiable instruments

Year	Number of declarations or disclosures (currency)		Suspicious cross border incidents
	Incoming	Outgoing	
2010	3	11	0
2011	7	6	0
2012	7	5	0
2013	3	13	0
2014	7	8	0
2015	3	9	0

280. The authorities refer to constitutional constraints (as a Crown Dependency) which affect the IoM's power to control its borders and exercise customs controls. Nevertheless, there are sufficient legal powers under the current legal framework, such as searches for cash, BNI, postal packets, etc., which could be used more frequently and effectively by the customs officers and constables to detect falsely or undeclared cross-border transaction of currency and BNI.

281. While the responsibility lies on the CED, being part of the EU customs union, the actual patrolling and enforcement actions are taken, when taken, by the Police. For example, in 2015 the IoM authorities reported that the police canine unit carried out 219 checks on incoming and outgoing baggage at the Sea Terminal, 16 of which were in conjunction with CED. There is no enforcement of disclosure requirements and no random searchers that are conducted on a routine basis. Nevertheless, the IoM authorities, as explained above, undertake occasionally exercises to detect drugs and cash. The IoM authorities also reported that such exercises could be carried out upon receiving good intelligence, though no successful examples were provided to the evaluators in this respect. One of the priorities for improvement that would enhance the effectiveness of customs controls on cash and BNIs is to enable the legislation to allow for targeted actions and controls on goods and cash entering or leaving the IoM, which is expected to introduce some enforcement measures of disclosure requirements. In 2015, the IoM was invited to join the UK national committee on cross-border cash declarations and seizures. This is expected to further improve the connections and facilitate the flow of information and intelligence between the counterpart authorities.

282. The CED has sufficient powers under CEMA and POCA to seize cash both where there is a suspicion of ML/FT/ predicate offences and where there is a false/non-declaration. In practice, however, if someone is found not to have declared cash but there are no other substantive reasons to suspect that either the origin or intended use of the cash is linked to unlawful conduct, the CED neither seizes, and as a result, nor forfeits the cash. The authorities indicated that without a suspicion, there may not be sufficient prima facie grounds for seizure of the cash. The evaluators were informed that even in those rare cases where a substantial amount of undeclared cash is detected, it would not be seized and forfeited.

283. Where there is a suspicion of unlawful conduct, the CED may seize the cash and detain it for 48 hours pending further investigation. It remains the case that it would have to be shown that the cash was the proceeds of, or intended for use in, unlawful conduct. This is also in line with Criterion 32.8, which states that competent authorities should be able to stop or restrain currency or BNIs for a reasonable time in order to ascertain whether evidence of ML/FT may be found. The person may still be subject to penalties, even if the cash were not ultimately forfeited. According to the IoM

authorities, a suspicion that could lead to seizure would arise, for instance, where a customer withdraws cash from a bank account with the intention to physically transport it outside of the IoM, the bank advises the customer that a declaration is required and the customer fails to do so. A SAR submitted to the FIU by a bank with respect to a cash withdrawal would provide even better grounds for seizure of the cash on the basis of suspicion. Nevertheless, from the cases presented to the evaluators, it appears that a mere SAR alone would not be sufficient. An additional confirmation given by the FIU on the legitimacy of the cash withdrawn would be one of the factors in determining whether to seize the cash. In a particular case given as an example, once the FIU confirmed that the withdrawal seemed to be legitimate, the circumstances were considered as not raising any suspicion concerning the unlawful origin or the intention for using the cash for criminal purposes. Also, no penalties were applied in this case.

284. The available information demonstrates that the confiscation regarding falsely or undeclared cross-border movements of currency and BNIs that are suspected to relate to ML/TF and associated predicate offence is not applied in the IoM as effective, proportionate and dissuasive sanction. There is also a very limited application of the powers to seize for further investigation of the cash or BNIs that are subject to none or false declaration/ disclosure. Although, police and Customs and Excise undertake intelligence-led operations targeting people, vehicles and cargo entering or leaving the IoM, as well as risk-testing exercises and other preventive measures, the efforts to detect such undeclared currency and BNI are limited.

Consistency of confiscation results with ML/TF risks and national AML/CTF policies and priorities.

285. The confiscation results achieved so far by the IoM do not appear to be consistent with the level of ML/TF threat present in the country and national AML/CFT policies and priorities. The IoM authorities do not pursue seizure and confiscation of criminal proceeds systematically and as a high priority criminal justice policy objective. The authorities do not proactively seek cooperation from their foreign counterparts in order to initiate restraint or confiscation of assets located or moved abroad while the main focus is given to seizures and confiscation of proceeds from local predicate offences.

286. The authorities acknowledged that given the nature of the IoM as an international financial centre where a significant volume of assets is held by FIs for corporate structures, those numbers may potentially be high. Nevertheless, the overall value of proceeds and instrumentalities of crime restrained, confiscated and actually recovered remains very low and though few ML investigations have been initiated with regard to suspicions in ML (for example, regulatory actions taken in one case led to 200 STRs involving ML suspicions related substantial amounts of assets, including unexplained wealth of individuals from Eastern European countries), none of them resulted in seizures or confiscation.

287. The evaluators are especially concerned regarding the lack of use of the non-conviction based asset recovery regime and the absence of systematic parallel financial investigations aimed at identifying potential criminal assets subject to confiscation.

288. Additionally, though the confiscation results reflect the IoM assessment of its FT risks, the assessors remain unconvinced that these reflect the actual risk of the IoM, as an international financial centre. Several cases were discussed on-site where FT suspicion was identified, however, was not properly reported or investigated, and no additional effort was made to identify and confiscate the assets related to FT. Such examples include positive matches of persons' property according to UNSC sanctions lists, as well as money transfers to or from high-risk jurisdictions.

289. With regard to confiscation of falsely or undeclared cross-border movement of cash/BNIs, even though the identified threats, according to the NRA, concern illicit cash, criminal property and drugs, the efforts to address these threats are limited. The main focus is placed on the detection of

prohibited items. Likewise, bearing in mind the limited measures in place to address the identified threats, the overall assessment of the associated risk appears to be unjustified. It also does not take into account the risk related to falsely or undeclared cross border cash and BNIs, existing in its neighbouring countries.

290. The authorities have indicated that efforts have been made with regard to enhancing the capacity of financial investigations aimed at detecting criminal assets, yet the confiscation results do not reflect these efforts.

Conclusion

291. **The IoM has achieved a low level of effectiveness for Immediate Outcome 8.**

CHAPTER 4. TERRORIST FINANCING AND FINANCING OF PROLIFERATION

Key Findings and Recommended Actions

Key Findings

Immediate Outcome 9

•

• The IoM draws upon the policies and work of the competent authorities in the UK with respect to combatting terrorism and FT issues,. Despite good relations with its UK counterpart authorities, as explained under IO 1, the IoM's understanding of foreign FT risks is not yet comprehensive enough, as it does not monitor high-risk situations (such as transactions to high-risk jurisdictions) at a national level.

• One shortcoming identified with respect to Recommendation 5 may potentially have negative effects on the effectiveness of the CFT-regime.

• The authorities have not yet detected any potential cases of FT and therefore have not yet had the opportunity to demonstrate the effective investigation and prosecution of FT. While the IoM draws on expertise provided by the UK security services and law enforcement, the IoM has limited domestic capacity and capability to detect and investigate FT suspicions. This concerns FT-related SARs, reported matches of targeted financial sanctions, especially those involving high risk jurisdictions, and incoming FT-related MLA requests.

• Limited exchange of information between the authorities involved in the prevention and detection of FT, the lack of relevant procedures as well as the absence of FT-specific guidance to financial institutions and DNFBPs, potentially hamper the taking of effective action.

• Insufficient training appears to have been provided to the authorities with FT competences.

• Although the IoM has addressed the risks posed by local NPOs, further work is needed with regard to the monitoring of additional potential FT-risks, such as those arising from financial activity of foreign NPOs and from transfers of funds to high risk jurisdictions.

Immediate Outcome 10 and Immediate Outcome 11:

• Since April 2016, TFS apply without delay. Several cases of detection and freezing of assets under FT TFS demonstrate their effective implementation. No PF-related assets or funds have been frozen.

• The general level of understanding of TF and PF-related TFS seems to be satisfactory among banks, This is not the case with respect to TCSPs, securities, insurance and on-line gambling operators. Also, (i) banks' use of the TCSP sector when on-boarding a customer that may not have been effective in the implementation of CDD measures; (ii) the fact that there have been several failings between

2012-2015 by banks to record all connected parties to their automated system (e.g. directors, trustees etc.); (iii) some smaller TCSPs' and online gambling operators' approach to screen customers against UN Resolution lists only when the customer is deemed high risk and therefore do not cover all clients, have a negative impact on the effectiveness of FT and PF-related TFS. Moreover, the authorities and the private sector were not clear on the steps that would be taken to manage assets held by complex structures should these be detected and frozen in the future.

• A positive aspect of the system is the widespread use of automated or manual screening systems (that rely on commercial databases such as World-Check, Dow Jones etc.) implemented by the majority of private sector participants. While the use of commercial databases is positive, however FIs and DNFBPs met on-site were not able to explain what additional measures would be taken to detect funds or other assets jointly owned or controlled, directly or indirectly, by designated persons or entities.

• Sectors other than banks have had limited or no supervision and monitoring. Moreover, there is insufficient guidance on how to apply FT and PF sanctions, as well as inadequate communication of new sanctions listings.

• While the authorities have provided a few positive examples of co-operation and co-ordination in the implementation of TFS, the assessors remain concerned by the lack of sufficient coordination between the CED, which is the competent authority responsible for the implementation of the UNSCRs, and the IOMFSA, the FIU and Police.

• A risked-based and proportionate regulatory regime for supervision of non-profit organisations has been introduced. However, it has not yet been fully implemented. Further work is needed with regard to the risk posed by unregistered NPOs which are not considered charities.

Recommended Actions

Immediate Outcome 9

• Conduct an assessment of existing cases and possible obstacles for properly addressing the risks through the investigations and prosecutions of FT.

• Adopt an independent CFT-strategy, from which a clear policy for tackling FT can be developed. The capacity of law enforcement authorities should be significantly enhanced.

• Ensure that FT investigations are carried out systematically upon suspicion of FT identified either by intelligence shared with the UK, by STRs, from incoming MLA requests, or in connection with reported action regarding targeted financial sanctions.

• Develop FT-specific procedures for providing real time guidance to financial institutions and DNFBPs in situations where a FT suspicion arises (e.g. "consent requests)"; such procedures should ensure the ability of all relevant competent authorities to take necessary coordinated investigative action, and avoid potential tipping off.

• Amend the legislation to remedy the shortcoming identified in criteria 5.2 of Recommendation 5.

Immediate Outcome 10 and Immediate Outcome 11

• Develop guidelines to: (i) for all FIs and DNFBPs on the identification of funds or assets wholly or jointly owned or controlled, directly or indirectly, by designated persons or entities and third parties; (ii) ensure that all the authorities and the private sector are aware of the steps to be taken when managing frozen assets held by complex structures, should these be detected in the future, for both FT and PF; (iii) strengthen the understanding by the TCSP, online gambling, securities and insurance sector of FT and PF-related TFS obligations.

• Enhance supervision of FIs and DNFBPs in relation to their compliance with obligations under FT and PF related TFS.

• Conduct outreach to ensure that smaller financial institutions and TCSPs are aware of FT risks.

• Establish clear lines of communication and adopt the necessary institutional arrangements between the competent authorities (Customs and Excise Division, IOMFSA, Police, FIU) to ensure effective implementation of TFS and a broader counter TF policy aiming at implementing possible criminal, civil or administrative processes beyond the freezing measures.

• Continue implementing the regulatory regime for supervision of non-profit organisations. Focus should also be given to the risk posed by unregistered NPOs which are not considered charities. Additional consideration should be given to FT risks, such as those arising from financial activity of foreign NPOs, and of transfers of funds to high risk jurisdictions.

• Establish a more proactive system to promptly notify reporting entities of new sanctions listings.

The relevant Immediate Outcomes considered and assessed in this chapter are IO9-11. The recommendations relevant for the assessment of effectiveness under this section are R.5-8.

Immediate Outcome 9 (TF investigation and prosecution)

292. The IoM has enacted a robust legal framework for combating FT, which is largely in line with international standards. However, one technical shortcoming remains, which relates to the financing of unproscribed terrorist organisations in situations when there is no direct link to a terrorist attack. This is because the offence of Facilitating Funding requires a subjective test of whether an individual had knowledge or reasonable cause to suspect or failed to exercise due diligence as to whether funds will or may be used for the purposes of terrorism (Part II of ATCA 2003 gives the list of proscribed organisations). This may potentially hamper the FT regime's effectiveness given the nature of the threat to the financial system in the IoM, which may potentially be abused for layering funds sent for "legitimate" activities of terrorists and terrorist organisations.

Prosecution/conviction of types of TF activity consistent with the country's risk-profile

293. The authorities have, to date, not detected any potential cases of FT and therefore have not had the opportunity to demonstrate the effective investigation and prosecution of FT. The assessment team considers that the absence of FT investigations or prosecutions can be explained, in part, by the lack of awareness and a proactive approach in cases of potential suspicions of FT. The assessors remain unconvinced that the potential TF threat is properly mitigated and therefore the absence of FT investigations and prosecutions is not consistent with the threat which the country faces.

294. As a Crown Dependency, the IoM's policies for combatting terror somewhat rely on those of the UK, and according to authorities good relations exist between the relevant counterparts. Nevertheless, the FT threats faced by the IoM as an international financial centre offering services worldwide including in high-risk jurisdictions are not comprehensively understood by the authorities, nor by its financial institutions and DNFBPs, for the reasons outlined under IO 1.

TF identification and investigation

295. Where national (i.e. UK-based or affecting the UK) or international terrorism is involved or suspected, the UK National Crime Agency ("NCA") or the British security services would be expected to be the lead agency for identification and investigation of FT suspicions. In the IoM, the police would be the lead agency. There is no local dedicated anti-terrorism unit. Additionally, there are no dedicated specialists within the IoM Constabulary or the prosecution service to deal with FT matters. Specialist training on countering terrorism was provided to law enforcement authorities, which contained a limited component on FT. While the IoM draws on expertise provided by the UK security services and law enforcement, the evaluators are of the view that the IoM has limited domestic capacity and capability to deal with this threat. The UK National Threat Assessment, and other information and trend indications provided by the NCA and security services contain some FT threat

information for the IoM. There has been one MLA request relating to terrorism or FT. No parallel financial investigations have ever been conducted in relation to terrorism or FT.

296. The evaluators were informed that the same types of powers and procedures, and the channels for the exchange of information, would be used in the investigation of suspected FT as would be employed in ML investigations. The channels to exchange sensitive information with the UK authorities have recently been strengthened.

297. Not enough evidence was presented by the authorities to demonstrate that they have properly detected and investigated possible FT suspicions. This is with regard to FT related SARs, reported matches of targeted financial sanctions especially in situations where these involve high risk jurisdictions, and one incoming FT related MLA request. During the onsite visit, the evaluators came across several examples where potential TF activities should have been at least considered for investigation and potential missed opportunities which were not pursued to support counter terrorism investigations.

298. As stated under IO 6, a number of notifications containing intelligence on FT were disseminated by the FIU to the FCU. However, it is not clear what action was taken with respect to these notifications.

299. Another potential source for FT investigation is in cases of asset freezing by FIs and DNFBPs due to matches found of TFS both when directly related to TF, or when involving high risk jurisdictions. Since January 2001, the CED has recorded a total of 50 sanctions enquiries labelled as "terrorism" (out of a total of 728 enquiries on sanctions matters recorded in just less than 14 years). The vast majority involved enquiries regarding checking potential or near matches, and one involved funds belonging to a UK-based father and son who were arrested in the UK but subsequently acquitted.

300. In discussions with the authorities there seems to be an understanding that once the assets are frozen, the IoM has fulfilled its international obligation, and accordingly the evaluators were surprised to be informed these occurrences were not additionally investigated for potential TF.

301. However, examples were given where the CED had proactively conducted enquiries following information coming to their attention, independently of any MLA request or enquiry or SAR from a local business. Such inquiries did not amount to a full FT criminal investigation of all parties involved though.

Case example: CASE – SRI LANKA
In November 2015, the CED identified the involvement of an IoM based business in the field of maritime security with persons in Sri Lanka about whom concerns had been raised in the local (i.e. Sri Lankan) media. Whilst no requests for information or assistance had been received from the Sri Lankan or the UK authorities, enquiries were initiated into the extent of the involvement. As the allegations made involved firearms and ammunition, and possible movement or use of such with proper authorisation, in a volatile part of the world, CED regarded it as important to establish the facts of the situation and to ensure that the IoM business was not involved or affected by any possible criminal activity. The IoM business holds a licence issued by the Treasury permitting the movement of firearms and related equipment, and the IoM thus has a direct interest in any potential problems that might affect the business. The business itself has been subject to background and other checks in both the IoM and the UK both prior to receiving a licence and subsequently. The case continues.

302. The IoM authorities provided the SRI LANKA case as a further example of how co-operation, advice or persuasion may serve to disrupt in cases where for whatever reason it was not possible or practicable to secure a conviction (for example, any persons or funds were outside the jurisdiction, and no apparently unlawful activity was being undertaken locally). In these cases there were

attempts to use the IoM companies in the complex corporate structures used to carry out and mask the crime. The IoM authorities emphasize that the co-operation between the CED and the TCSP affected, with the former providing advice, information and assistance to the latter, meant that the number of such companies that were successfully established was few. In at least one case, involving suspected VAT fraud, this co-operation also led to a large sum of money (up to £3 million) that would have been paid to a suspected fraudster being blocked and recovered. The FIU also encouraged similar co-operation, and both the CED and the FIU would always seek to assist compliance staff and the like, wherever possible.

303. While the evaluators commend the IoM authorities for their cooperation with foreign jurisdictions on these sensitive matters, they find less positive the fact that apparent instances, which seem to have potentially been perpetrated as part of the layering process of various terror financing cases, were not considered or investigated as such.

The international aspect

304. Another potential source of FT-related suspicions is international co-operation. In the period under review, only 1 terrorism related MLA was received (in 2011).

305. In the absence of reliable statistics on financial inflows and outflows through the IoM `s economy, it is currently unknown where funds are actually transferred to, i.e. high-risk jurisdictions, jurisdictions and areas bordering with such and jurisdictions cooperating with high-risk jurisdictions. This issue was discussed during the on-site with various authorities as financial links to high risk jurisdictions worldwide are not uncommon as illustrated anecdotally by several cases. This issue was identified in the NRA and steps have been initiated by the authorities to rectify the situation.

FT suspicious activity reporting

306. The IoM authorities assured the evaluators that any SAR received by the FIU that involve reasonable grounds to suspect FT or terrorism links would be referred to the police and to the security services in the UK. The same would apply to any other intelligence or other information received regarding FT.

307. When examining with the authorities a recent on-going FT SAR analysis regarding an extremely sensitive suspicion of FT involving both the UK and the IoM, the evaluators were surprised to find that the FIU had disseminated to the Special Branch of the police only a partial and sanitized version of that SAR. The SAR was then forwarded to UK NCA but without enough detail or any added analysis. The officer handling this case had not received any specific FT training. No special instructions were given to the relevant financial institution, and no investigative steps had been initiated by the authorities.

308. A case was investigated where a link was identified between a drug trafficker and a friend thought to have been radicalised. While the authorities seem to have properly addressed the risk of radicalisation, they did not look into whether the drug trafficker may have potentially funded his friend or other FT links. The information provided on this issue to the evaluators seemed to be anecdotal but deserves attention due to the gravity of the potential threat of such ties.

309. The evaluators were additionally left with some concerns when discussing the issue of potential FT suspicions with representatives of the private sector. Private sector representatives described examples where attempts were made to set up structures in the IoM to get around sanctions in Iran. Such attempts were detected and reported but no investigative effort seems to have been taken with regard to investigating potential ML or TF suspicions.

TF investigation integrated with -and supportive of- national strategies

310. There is no IoM overarching national strategy for the combatting of terrorism and specifically FT, and the relevant National Threat Assessment for terrorism would be that prepared by the UK authorities. In respect of sanctions, the CED co-operates closely with both the FIU and Her Majesty's Treasury (UK) and, where any information relating to actual or suspected terrorist activity is discovered, including any suspected financing or laundering of funds, this would be supplied to the police and/or HM Treasury and UK NCA.

311. The CED now has a seat on the UK NCA-led national co-ordinating body (known as CIG) concerned with cash declarations and cash seizures throughout the UK. The police also have close links with the UK NCA, and are negotiating a formal memorandum of understanding to place co-operation and exchanges of information between them on a more formal footing.

312. Nevertheless, the evaluators are of the opinion that insufficient measures are taken by the IoM authorities to identify, initiate and prioritise FT cases to ensure prompt investigation and action against major threats and to maximise disruption. While a number of measures have been taken to enhance the capacity and the capability of law enforcement authorities concerning FT investigations, the authorities have no specific policy or strategy to deal with particular FT threats and trends. This is not consistent with the FT threat the IoM faces as an international financial centre.

313. The IoM authorities do not systematically and promptly obtain and access relevant financial intelligence and other information required for FT investigations and could not demonstrate the underlying considerations for decisions made not to initiate a criminal FT investigation, even when appropriate.

314. The exchange of information between the relevant authorities involved in prevention and detection of TF does not always occur, and in many cases information held by the CED, the FIU, the IOMFSA or the police, regarding potential FT suspicion was not made available to the other relevant competent authorities.

315. The authorities are encouraged to adopt as part of their CFT strategy appropriate procedures for interagency co-operation on FT issues, the absence of which hamper the effectiveness of the IoM's CFT system. To date the strategy is not fully functioning coherently to mitigate its terrorist financing risks. The authorities should also properly co-operate and co-ordinate their respective tasks associated with IO 9.

316. As part of their CFT strategy the authorities are additionally encouraged to introduce more specific TF guidance to financial institutions and DNFBPs.

Effectiveness, proportionality and dissuasiveness of sanctions

317. As there have been no FT prosecutions and convictions the evaluators are unable to assess whether sanctions or measures applied against natural and legal persons convicted of FT offences are effective, proportionate and dissuasive.

Alternative measures used where TF conviction is not possible (e.g. disruption)

318. As described above the authorities have in several cases proactively taken preventative measures with regard to FT. However these measures have been used randomly based on best knowledge and the will of relevant institutions, and not in a strategic way.

Conclusion

319. **The IoM has achieved a moderate level of effectiveness for Immediate Outcome 9.**

Immediate Outcome 10 (TF preventive measures and financial sanctions)

Implementation of targeted financial sanctions for TF without delay

320. The IoM is not a member of the United Nations ("UN") in its own right, although it is permitted to implement UN obligations within the IoM. The UK remains responsible for any shortcomings in the IoM's compliance with the UNSCRs and the IoM relies on the UK's policies for combatting terrorism/TF, identification of TF risks and the application of counter-measures.

321. Legislative amendments were brought into force in order to implement targeted financial sanctions ("TFS") without delay, in compliance with UNSCR 1267, it successor resolutions and UNSCR 1373. Under the new provisions of the Terrorism and Other Crime (Financial Restrictions) Act ("TOCFR") of 2014, which entered into force only recently, all UK lists have been automatically incorporated into the IoM's freezing regime. In practical terms, this means that any UN, EU, or UK specific designations (once in force in the UK) would have a direct effect in the IoM. Before the recent law came into force, as an interim solution, the Treasury (CED) could amend the list implementing the relevant UNSCRs, by its order, which speeded up the process.

322. A mechanism is in place for domestic designations pursuant to UNSCR 1373. However, it has never been applied in practice.

323. There have been 4 terrorism-related matches, 3 under EU 2580/2001 and 1 related to a designation under the UNSCR 1267 (Qadi). In 3 other cases, assets were frozen as they were potentially linked to terrorism. 32 other matches relate to other country-based sanctions, some of which involved persons located in jurisdictions considered as posing a higher FT risk. While this assessment is not concerned with the implementation of these other sanctions, the evaluators consider these matches a positive indication of the effective implementation of TFS.

324. The automatic implementation of the lists, together with the examples of assets frozen under TFS, illustrate the efforts of the authorities and the private sector to prevent the flight or dissipation of funds or other assets which are linked to terrorists or terrorist organisations. However, notwithstanding the cases of detection, the awareness of the obligations under the UNSCRs is uneven. The general level of understanding seems to be satisfactory among banks, This is not the case with respect to TCSPs, securities, insurance and on-line gambling operators. The private sector did not know what steps needed to be taken should assets held by complex structures be detected in the future (e.g. appointing a receiver to hold the shares, court-appointed directors to manage the activities of the company, etc.). The authorities were not familiar with such procedures either.

325. The mechanism for communicating designations to FIs and DNFBPs relies on the publication of the UNSCR lists in a dedicated area on the CED's website. Entities can subscribe to a CED feed that will send out details of such news releases (which average around one per week). However, subscription to this news feed is not mandatory. In addition to the news feed, the "VAT Notes" sent to all VAT-registered businesses in the IoM on a quarterly basis can also contain information relating to sanctions and similar matters. Furthermore, the IOMFSA publishes press releases with links to the CED's website and issues a quarterly bulletin which contains information on freezing obligations and relevant updates, including new designations. Apart from the above-mentioned information sources, there are no other mechanisms in place to ensure the prompt transmission of designations, freezing obligations and other relevant updates. As a result, there may be situations where some FIs or DNFBPs may not be aware of new designations, especially those which do not subscribe to the CED feed. The authorities are not in possession of information on which entities have not subscribed to the feed.

326. A positive aspect of the system is the widespread use of automated or manual screening systems (that rely on commercial databases such as World-Check, Dow Jones etc.) implemented by the majority of private sector participants. While the use of commercial databases is positive, FIs and DNFBPs met on-site were not able to explain what additional measures would be taken to detect funds or other assets: (i) that are jointly owned or controlled, directly or indirectly, by designated persons or entities; (ii) that are derived or generated from funds or other assets owned or controlled, directly or indirectly, by designated persons or entities; or (iii) of persons and entities

acting on behalf of, or at the direction of, designated persons or entities. Additionally, the private sector did not appear to acknowledge that the application of CDD is an essential component in complying with TFS obligations. They indicated that the screening process sufficiently covers the requirements to detect designated persons. This might be understandable bearing in mind that the definition of funds under the freezing obligation was extended only recently to assets that are jointly or indirectly owned, held or controlled.

327. Issues may also arise with respect to banks' use of the TCSP sector when on-boarding a customer. TCSPs may not have been effective in the implementation of CDD measures, such as effectively undertaking CDD on the ultimate beneficial owner (see IO 4). Additionally, there have been cases where banks have failed to connect all parties to their automated system (e.g. directors, trustees etc.) ultimately preventing all parties to be screened appropriately (see IO 4). The IOMFSA's themed visit programme (2012 to 2015) found that banks had, in some cases, failed to record all connected parties of the customer on their systems, e.g. directors, shareholders, beneficiaries, etc. As a result, there will have been cases where not all persons connected to a particular relationship have been screened on an on-going basis. Findings were subsequently remediated. Some market participants (especially some smaller TCSPs and online gambling operators) screen customers against UN Resolution lists only when the customer is deemed high risk and therefore do not cover all clients. For example, one online gambling operator, having a material market share, only screened clients against UN Resolution lists when meeting other high risk criteria) until the beginning of 2016. The GSC confirmed that this shortcoming has now been rectified.

328. Discussions with the industry indicated that no or limited guidance is provided on the implementation of UNSCRs. While in theory FIs and DNFBPs would have to report the freezing of funds to the CED, this is not always the case. Some FIs and DNFBPs (including TCSPs, insurance and securities sector participants), which pose an above average ML/TF risk to the IoM and with a material contribution to the IoM's economy, stated that they would only report to the FIU. This ultimately shows that not all private sector participants have been made aware of which authority is responsible for the implementation of TFS and to whom information about freezing of funds or assets must be submitted. Lack of clarity also remains as to when a match with a designation should lead to the submission of a SAR. The evaluators were also not convinced that reporting entities would report attempted transactions (as required under c.6.5(e)).

329. In terms of supervision, the discussions with the industry revealed that the monitoring and the control activities are often limited to the implementation of the sanctions based on the screening exercise. No additional measures are taken to ensure that no funds or assets are made available, directly or indirectly, or for the benefit of the designated persons or entities. Banks and the supervisor confirmed that their automatic screening mechanisms and payment systems are checked by the IOMFSA during on-site visits for sanctions. The insurance sector, the securities sector and TCSPs did not confirm that they have been subject to any monitoring or supervision with respect to the TFS. There has been a limited number of supervisory visits by the GSC and by SRBs (such as law society ICAEW and ACCA) with respect to these requirements. In addition, the IOMFSA is not always informed of matches reported to the CED, which hampers the ability to properly supervise the implementation by FIs' and DNFBPs' obligations. This amongst other factors causes a lack of understanding on the steps to be taken and what measures are to be implemented whenever a match to one of the lists is reported.

330. While the authorities have provided a few positive examples of co-ordination and co-operation, the assessors remain concerned by the lack of sufficient coordination between the CED, which is the competent authority responsible for the implementations of the UNSCRs, and the IOMFSA, FIU and Police. This results in the lack of understanding on the steps to be taken and what measures are to be implemented whenever a match is identified. The cases when funds or assets were frozen pursuant to the UNSCRs, or other country-related sanctions, were not further analysed by the CED in order to identify some potential cases to be submitted to the FIU/FCU for further

investigation into possible FT. However, the authorities do cooperate with the UK HM Treasury. They referred to a case where a UK SAR connected to sanctions with an IoM link, was consulted on between the UK Treasury, the CED and the FIU.

Targeted approach, outreach and oversight of at-risk non-profit organisations

331. A review of the NPO sector in relation to the FT risks was undertaken in 2014. The review resulted in identifying the NPOs which are at a higher risk – Specified NPOs (SNPOs). Subsequent legislative amendments were made to bring the NPOs which fulfil the specific requirements established by the POCA 2008 within the regulated sector (see criterion 8.1).

332. NPOs are required by law to determine whether they fall under the category of SNPOs. Nevertheless, to date, NPOs do not appear to have done so. Instead, the IOMFSA was in the process of identifying and registering those NPOs.

333. Out of the 50 charities that have been identified as being able to send money to higher risk jurisdictions, 11 entities were initially identified, upon discussion with those, as SNPOs and 3 were outside the scope. Of the remaining 8, 1 was dormant and 1 appeared to be remitting funds to the UK, and not high risk jurisdictions. The remaining 6 were registering or had been registered as SNPOs.

334. Though registration requires the submission of details of any of the persons who can be considered specified persons, in practice, the IOMFSA seeks to register the details of all the relevant persons controlling or directing the activities or the assets at the disposal of the SNPOs, which is a positive aspect of the system. The IOMFSA has undertaken active measures to require such information from SNPOs which applied for registration. However, to date, not all of them have provided the requested details and, subsequently, these are not available in the IOMFSA's registry. This is because at the time of the on-site visit the process was still under way.

335. A risk assessment conducted specifically with respect to the NPO sector in 2014 identified the FT risk related to the NPO sector as low. Nevertheless, the risk analysis performed by the authorities only took into account information available in the Central Registry on registered charities. Other NPOs were considered insignificant for the purposes of supervision. Such an approach could have led to the exclusion of NPOs that are not charities (but religious, social, etc. as per objective) from registration and supervision. Though the authorities believe that such NPOs do not currently exist, the potential of unregistered NPOs to be involved in FT may exist in the future and therefore the evaluators believe that the authorities should consider registering all NPOs to monitor the transfer of funds to high risk jurisdictions. Risk posed by the 6 exempted charities, which are not registered in the Central Registry and not monitored by the IOMFSA, were only partially analysed.

336. Two outreach activities have been carried out. The first was conducted by the IOMFSA in conjunction with the Central Registry, for all charities (2014) and the second was conducted by the IOMFSA, targeting only the potential SNPOs (2015). Further outreach activities have already been planned and it appears that the outreach efforts will be carried out on a systematic basis. An AML/CFT Handbook which includes a section dedicated to SNPOs is available for this newly regulated sector.

337. As there was no effective supervision yet at the time of the on-site visit, the authorities were still unaware as to what extent NPOs have implemented the elements required by Recommendation 8 and, specifically, the "know your beneficiary and associated NPOs" rule, with regard to both UK NPOs and those established in high risk territories.

Deprivation of TF assets and instrumentalities

338. In practice, the IoM has effectively frozen and deprived terrorists, terrorist organisations and terrorist financiers of their assets only in cases matching the persons/organisations listed under

UNSCRs. It has not been demonstrated that a proactive approach has been taken to implement criminal, civil or administrative processes beyond the implementation of UNSCRs.

339. It was also noted that SARs have not always been filed where a match with persons/entities listed in a UNSCR was identified. As a result investigations have not been initiated, nor have outgoing international requests been sent in relation to these matches. Subsequently, no additional assets have been deprived from terrorist, terrorist organisations or terrorist financiers.

340. The lack of an overarching policy on the cooperation between the relevant authorities involved in prevention and detection of TF has an impact on the IoM's capacity to deprive terrorist organisations and terrorists of assets and instrumentalities.

341. FT specific guidance to FIs and DNFBPs is not detailed enough. The capacity of the authorities with FT competences appears to be limited and limited training has been provided with regard to TF.

342. On a positive note, although the UK is responsible for foreign policy matters, the IoM has introduced a procedure in Part 4 of the TOCFR 2014 whereby any person affected by a decision of the Treasury relating to a freezing order or a direction under UN Measures, can apply to the High Court for the decision to be set aside (this is supplemented by several possibilities to turn to UN Sanctions Committee, Council of European Union and Court of Justice of the European Union).

343. Applications for the release of funds where certain conditions are met (e.g. humanitarian issues, development purposes, etc.) are administered by the CED, which consults on applications with HM Treasury (and/or any other appropriate agency) before making a recommendation to the Treasury. Any licence is signed by the Treasury Minister.

Consistency of measures with overall TF risk profile

344. The assessors remain unconvinced that the authorities' view that FT risk is medium to low reflects the actual position in the IoM, particularly since as an international financial centre, the IoM is exposed to enhanced threats. The evaluators identified several cases in which a suspicion of FT arose, but which was not properly reported or investigated and where no additional efforts were made to identify and confiscate assets related to FT. Such examples include positive matches of persons under terrorism-related UNSCRs, matches with UNSCRs related to countries which are of high FT risk, and money transfers to or from high risk jurisdictions.

345. Awareness of FT risks and UNSCR obligations in all the sectors, other than the banking sector seems to be low. For example, no discussions seem to be held within the insurance industry, notwithstanding the fact that insurance policies have been detected and reported under the TFS regime.

346. The lack of discussions and awareness raising appear to have affected the input of the relevant sectors into the NRA and the evaluators remained concerned that these risks have therefore not been explored by the competent authorities.

347. In addition, further work is needed by the competent authorities to consider additional FT risks, such as those arising from financial activity of foreign NPOs, and of transfers of funds by all these to areas of conflict, as well as the risk posed by unregistered NPOs.

Conclusion

348. **The IoM has achieved a moderate level of effectiveness for Immediate Outcome 10.**

Immediate Outcome 11 (PF financial sanctions)

Implementation of targeted financial sanctions related to proliferation financing without delay

349. The mechanism implementing proliferation-related TFS is the same as the one for FT.

350. All the relevant UNSCRs (those relating to North Korea and Iran, as well as UNSCR 1540 on the non-proliferation of WMD) are given effect under the TOCFR 2014 and are applied, as from 2007, by means of the application of the corresponding EU Regulations. As the IoM also applies UK export and trade control law, procedures and controls on exports of dual-use items and technology are also applied. Where these are imposed because of the UK's (or the EU's) commitments under various international agreements (such as the Nuclear Proliferation Treaty and the Wassenaar Arrangement on dual-use goods and technology), the IoM would comply with those commitments even if any relevant treaty or agreement had not been extended to the IoM.

Identification of assets and funds held by designated persons/entities and prohibitions

351. The mechanism for communicating designations to the financial and non-financial institutions and for the identification of assets and funds held by designated persons and entities is described under IO 10. Any effectiveness issues identified also apply to the PF-related regime.

352. In the case of Iran, FIs have been compelled to consider any customer with a link to Iran as a potential money launderer or posing a PF threat. A requirement was introduced in January 2011 to notify, or seek prior authorisation for, transfers of funds to and from Iran and certain Iranian entities. As a result, in 2011 the CED processed 118 notifications with an overall value of £7.53 million, in 2012 the corresponding numbers were 38 and £8.08 million, in 2013 13 and £1.45 million and in 2014 14 and £1.15 million. In all cases, the CED authorised the carrying out of the transactions. However, before any funds requiring authorisation were permitted to proceed, checks were carried out, including the use of available open source material, such as World-Check, or further enquiries made with the applicants.

353. No assets or funds have been frozen under PF-related UNSCRs.

354. The CED deals with export and trade control licensing and investigates any suspected breaches. According to a Customs and Excise Agreement between the IoM and the UK, there is a requirement for the IoM to maintain its export controls so that they correspond to those in force in the UK. Therefore all export and trade control licence applications (except for cultural goods) are made via the UK Export Control Organisation by using that organisation's online 'Spires' system. The IoM does not maintain international trade statistics. Figures for IoM trade form part of the UK statistics (as the two operate a single customs area). There is little evidence of any significant trade or business involvement with DPRK. However, there was, prior to the increased UN/EU sanctions, some business involvement with Iran, including a large number of IRISL ships being owned through IoM companies. The CED is also aware of some business with Iran that has arisen following relaxation of the sanctions regime, in particular involving the shipping and oil sector, as well as enquiries relating to other smaller sectors, such as the supply of juvenile fish for farming.

FIs and DNFPBs' understanding of and compliance with obligations

355. The general level of understanding of PF-related obligations seems to be satisfactory among banks. Banks were also aware of their obligation to screen payments to understand their connection to PF. This is not the case with respect to TCSPs, securities, insurance and on-line gambling operators. All of the effectiveness issues raised under IO 10 with respect to the understanding and compliance with FT-related TFS, as well as the provision of guidance, also apply in relation to PF (see paragraphs 324 to 328).

Competent authorities ensuring and monitoring compliance

356. The AML/CFT Strategic Group has been set up to coordinate policymaking and provide a platform for cooperation between the domestic authorities, including PF issues. The assessment team had sight of the minutes of the Strategic Group which show that PF issues have indeed been

discussed. However, it appears to the evaluation team that no major co-operation issues were discussed. Most discussions appear to have been about how to improve legislation in this area and enhance information provided on the relevant government website. Moreover, the majority of the group participants were not aware of FATF best practices paper "Sharing among Domestic Competent Authorities Information Related to the Financing of Proliferation". Correspondingly, similar co-operation issues which are highlighted under IO 10 are relevant for PF-related TFS (see paragraph 330).

357. The authorities did however refer to a case in 2009 (before UN PF-related sanctions came into force) related to the Islamic Republic of Iran Shipping Line (IRISL), which had acquired a number of vessels through companies set up in the IoM. The vessels were registered on the IoM's shipping register, being reflagged back out to Iran (and hence flying the Iranian flag, with all operational control being in the hands of their Iranian owners). A local CSP was involved, but the business relationship had been formed long before any sanctions had been put in place. In response to sanctions imposed by the USA, the CED cooperated with the FIU, the HM Treasury in the UK, the CSP and US Treasury Office of Foreign Asset Control and as a result the CSP terminated the relationship with IRISL. The authorities presented this case to demonstrate that co-operation gateways are in place and are used effectively when the need arises.

358. As far as supervision is concerned, the same effectiveness issues identified with respect to IO 10 also apply here (see paragraph 329). In addition to the supervision by the FI and DNFBP supervisors, with respect to PF-related obligations, the authorities stated that the CED conducts audit visits to VAT-registered businesses in connection with customs and excise, or export and trade control licensing matters. Some of the VAT-registered entities may be licence-holders with the IOMFSA or GSC. The visits are primarily for the purposes of VAT etc. The authorities stated that CED officers are made aware of requirement of certain businesses to comply with the relevant AML code and would monitor the compliance by entities. Conclusion

359. **The IoM has achieved a moderate level of effectiveness for IO.11**.

CHAPTER 5. PREVENTIVE MEASURES

Key Findings and Recommended Actions

Key Findings

• The IoM has made significant efforts to understand its ML/TF risks, especially by conducting a formal NRA process. However, some areas appear not to have been subject to a sufficiently detailed analysis, and understanding of external threats is limited by the absence of some data. This affects the private sector's understanding of ML/TF risk.

• FIs and DNFBPs generally demonstrated knowledge of requirements of the AML/CFT Code. However, a number of deficiencies were noted, e.g. customers are not always asked upfront for information that will facilitate identification of PEPs, close associates or family members of PEPs, and there are some examples of TCSPs failing to undertake full CDD on beneficial owners.

• FIs and DNFBPs apply a risk-based approach, and hence apply enhanced CDD for higher risk customers. However, compared to the risks that are inherent in the Isle of Man's business model, the number of customers assessed by some FIs and DNFBPs as presenting a higher risk appears to evaluators to be low. Evaluators are concerned that enhanced CDD, including monitoring, will not be applied in any cases where customers that actually present a higher ML/TF risk are not rated accordingly. Moreover, there is a lack of guidance in the AML/CFT Handbook on the enhanced CDD measures to be applied where customer risk is assessed as being higher, including corroboration of source of wealth.

• ML/TF risks are not fully managed where a customer (an intermediary) acts on behalf of another customer. This is because: (i) FIs do not consider the risk profile of underlying customers due to statutory CDD exemptions granted in this area; and (ii) requirements to test that intermediaries are meeting requirements set in the AML/CFT Code are not always followed.

• The role that is played by third parties (non-eligible introducers) in the application of measures to verify identity is not clear, given the differing evidence presented to the evaluators. In particular, evaluators are concerned that some use is made of evidence of identity collected and/or held by third parties outside of the comprehensive regulatory regime that is applied to eligible introducers. Moreover, some FIs (particularly banks) and DNFBPs use CDD information presented by a third party (especially TCSPs that present the greatest inherent ML/TF risk to the IoM) that has collected this information in turn from another party – an "information chain". Because of this chain, there is an increased inherent risk that a FI or DNFBP may be provided with incomplete or false information and so unable to understand the nature of its customer's business and its ownership and control structure. If information is incomplete or false, then this will also affect on-going monitoring. Banks may be able to mitigate this risk through terms of business, but evaluators are not in a position to form a view on what is happening in practice and what effect this may have.

• The quality of SARs is rather low, with less than one third based on suspicion of ML/FT or underlying criminality.

• FIs and DNFBPs regulated under the FSA 2008 and IA 2008 are required to have an independent audit function, but not all securities firms have established such functions. There is no similar requirement in the AML/CFT Code (for other FIs and DNFBPs) or Online Gambling Code. Accordingly, such functions are not always found in online gambling operators. Where in place, e.g. life assurance companies, they do not always cover AML/CFT issues.

Recommended Actions

• Taking account of risk, authorities should further limit the circumstances in which CDD information and evidence of identity presented by a third party can be used, including where that third party has collected information from another party (an information chain). In particular, additional guidance should be provided by the IOMFSA to explain its expectations when use is made by FIs and DNFBPs of evidence of identity presented by non-eligible introducers, and training provided thereon.

• Authorities should require FIs to take account of risks presented by underlying customers when applying CDD exemptions to intermediary customers under paragraph 21 of the AML/CFT Code. Application of the exemption should also be prohibited where specific higher risk scenarios apply. Requirements to sample-test whether CDD and record-keeping requirements are appropriately applied to underlying third parties should be reviewed and alternative measures put in place, as necessary, to mitigate risk.

• Authorities should require FIs to assess whether to: (i) have sight of documents, such as letters of wishes, to determine who the ultimate beneficial owner is of a trust; or (ii) collect appropriate assurances from TCSPs (and keep evidence) that information in relevant documents (such as the letter of wishes) is consistent with information provided on beneficial ownership.

• Authorities should continue to work with FIs and DNFBPs to increase the quality of STRs with a view to improving the quality of disseminations, and provide greater feedback on the quality of STRs submitted.

• Supervisors should compare categorisation of risk by FIs and DNFBPs in order to be satisfied that they are consistent with the NRA and sectorial risks, and enhanced CDD measures are applied when required. Additional guidance should be provided, as appropriate, including on what may constitute a higher risk (taking into account risks that are inherent in the IoM's business model) and the enhanced CDD measures to be applied, including corroboration of source of wealth.

• Supervisors should provide additional guidance, and place further emphasis, on how to identify PEPs, close associates and family members of PEPs. Authorities should consider providing additional guidance to address other issues identified in this preventive measures section.

• Authorities should require all FIs and DNFBPs, taking account of risk and size of business, to: (i) have policies, procedures and controls for an independent audit function to test the AML/CFT system; and (ii) appoint a compliance officer.

• Other technical deficiencies (listed in the TC annex) relating to preventive measures should be addressed.

The relevant Immediate Outcome considered and assessed in this chapter is I04. The recommendations relevant for the assessment of effectiveness under this section are R9-23.

Immediate Outcome 4 (Preventive Measures)

360. The types of services and products offered by FIs and DNFBPs make the IoM attractive to non-resident customers, including high-net-worth individuals ("HNWI") wishing, amongst other things, to structure their assets in a tax efficient manner. Indeed, many of the financial services sub-sectors feature business models which specifically target non-resident HNWIs – in particular the TCSP and banking sectors. As a result, the vast majority of financial services offered have an international nature, some of which will be "politically exposed" and expected to increase risks of receiving the proceeds of foreign corruption or organised crime, and wealth management will include the use of complex, multi-jurisdictional ownership structures. Much of the non-retail financial business carried on in FIs and DNFBPs is non-face-to-face and conducted via professional intermediaries, including group entities, lawyers and independent financial advisors. Consequently, the IoM is considered by the assessors to have higher inherent risk characteristics.

361. At the other end of the risk scale there are high value dealers operating in the IoM, and accountants who do not handle customer funds and transactions. Moreover, the land-based casino and MSB providers also represent small sectors compared to other groups on the IoM.

Understanding of ML/TF risks and AML/CTF obligations

362. Each FI and DNFBP met on-site confirmed that an overall business risk assessment would be carried out. This assessment would assess: (i) the nature, scale and complexity of the institution's activities; (ii) the products and services provided by the institution; (iii) the persons to whom and the manner in which the products and services are provided; (iv) use of third parties to carry out elements of the customer due diligence process; and (v) technological developments. In the business risk assessment, or in a separate document for some, an overall risk appetite is also set. Such an approach provides a strong basis for the application of a risk-based approach to AML/CFT obligations.

363. Consistent with this finding, it was clear that risk-based decisions had been taken by a number of service providers to restrict or exclude some business lines (linked to over-arching risk appetite) and to apply additional conditions or documentary requirements for others. For example, in accordance with their risk appetite, there are some banks that will not provide products or services to crypto-currency (e.g. Bitcoin) operators, online gambling operators, or some TCSP client companies[39].

364. However, when some private sector businesses (including TCSPs and life assurance companies) described their risks to evaluators, it was apparent that, whilst aware of the risks inherent in the Isle of Man's business model, they were still unsure how their particular institutions

[39] However, not all banks exclude online gambling operators and TCSPs, hence these sectors are not excluded from the financial sector.

could be used in practice for ML and TF, despite having prepared business risk assessments. Moreover, banks' understanding of their customer portfolio was incomplete, because, in several cases, they did not hold management information about which countries they were receiving wire transfers from or sending wire transfers to. The absence of this management information may prevent FIs identifying TF threats that they face where customers are from areas of conflict, or from countries that are adjacent to such areas.

365. The IoM has made significant efforts to understand its ML/TF risks, especially by conducting a formal NRA process. However, the private sector's understanding of risk more generally is affected by the fact that, according to IO 1, some areas appear not to have been subject to a sufficiently detailed analysis, and understanding of external threats is limited by the absence of some data.

Application of CDD exemptions to underlying customers

366. The application of CDD exemptions by certain FIs to intermediary customers (customers that are subject to, and supervised for compliance with, AML/CFT laws and regulations (or equivalent standards in other jurisdictions) and acting for and on behalf of their own customers) is found in many countries. The effect of this exemption is that information on underlying customers is not disclosed upfront by the regulated intermediary to the FI. Risks inherent in such an exemption may be even higher in the IoM because such intermediaries are more likely to be non-resident, given the international nature of the IoM's business. Recognising this, inter alia the AML/CFT Code: (i) strictly regulates the circumstances in which the exemption can be applied; (ii) requires terms of business to be in place; (iii) unlike in many other jurisdictions, mandates testing of CDD applied by the regulated intermediary to its customers; and (iv) requires reasonable measures to be taken to ensure that evidence produced by the regulated intermediary in testing is satisfactory (which should include conducting a review of the intermediary's policies and procedures).

367. Despite the above, ML/TF risks are not fully managed. There are two reasons for this. First, FIs are not explicitly required to consider the profile of underlying customers, and so the majority of FIs interviewed were not aware of the actual profile of the ultimate customer base and the risks presented, and hence could not refuse to open an account if this was not in line with their risk appetite[40]. Second, evaluators were also told that, contrary to the AML/CFT Code, some regulated intermediaries (global firms established mainly in EU Member States) acting on behalf of their customers would present CDD information and evidence of identity for that customer only when: (i) there is a suspicion of ML or TF; or (ii) there is a legal requirement to do so, and not when called on to do so under terms of business (because such terms of business are not commonly found elsewhere). This means that FIs are not able to take steps to satisfy themselves that CDD and record-keeping requirements applied by their customer (the regulated intermediary) are in line with R. 10 and 11 by way of testing. One on-going investigation of potential money laundering highlights the risks involved. In this particular case, a pooled bank account was operated by a law firm and was used to transfer unusually large amounts of money – which were not picked up by the bank. In addition, the exemption may still be applied in any case where the regulated intermediary is assessed by the FI as presenting a higher risk of ML/TF.

Information chains

368. Interviews with banks highlighted cases where business may be introduced to the bank (and CDD information collected) by a TCSP which in turn had collected that CDD information from another third party, for example, from a local or overseas law firm. According to the NRA, non-face to face business is common and many TCSPs take on business from professional intermediaries, e.g. law firms, without meeting their customer(s) (or beneficial owner(s)). It was identified that these

[40] The IOMFSA has pointed to paragraph 21(2)(c) of the AML/CFT Code which requires a FI to know the nature and intended purpose of the business relationship. Evaluators do not consider that the effect of this provision is to clearly require FIs to consider the profile of underlying customers.

information chains are features of both the eligible[41] and non-eligible introducer regimes in other sectors too.

369. Where there is such a chain, risks increase. In particular: (i) the person originally collecting CDD could be twice or even further removed from the bank (before a TCSP there could be a local law firm, then an overseas law firm etc.); (ii) that person may not have applied CDD measures in accordance with the AML/CFT Code or international standard; and (iii) the bank would not know whether the customer (and/or ultimate beneficial owners) had been met face-to-face at some point in the chain. Accordingly, the bank may be provided with incomplete or false CDD information and not able to understand the nature of its customer's business and its ownership or control structure[42]. Banks may be able to mitigate this risk through terms of business, but evaluators are not in a position to form a view on what is happening in practice and what effect this may have.

Introduced business

370. The authorities have explained that a FI or DNFBP may meet the requirement in the AML/CFT Code to verify the identity of a person by: (i) placing reliance on identification measures already conducted by an "eligible introducer"[43] (third party in the sense that is to be understood under R.17) in line with paragraph 23 of the AML/CFT Code; or (ii) itself collecting evidence afresh.

371. The majority of FIs and DNFBPs interviewed on-site stated that they collect evidence afresh themselves, or, particularly in the case of the life insurance sector, the collection of CDD measures is delegated to IFAs in accordance with terms of business between the life assurance company and the IFA. However, one large bank that provides services to TCSPs explained that it would collect evidence of identity already held, and passed to it, by non-eligible introducers, and a second explained that evidence of identity for non-higher risk customers would be held on its behalf by non-eligible introducers (i.e. not called for upfront). Evaluators are of the opinion that this second situation points to the fact that reliance is being placed on a third party - in the sense that is to be understood under R.17 - to perform certain elements of CDD measures.

372. In addition, two banks that provide services to TCSPs also explained that they would be content to use evidence of identity provided by a TCSP that, in turn, had collected that evidence from another party (an evidence chain). In the securities sector, evaluators were also told that there had been some cases where, when asked for CDD information and evidence of identity, eligible introducers had been slow to forward this information or evidence, suggesting that they may have, contrary to the AML/CFT Code, relied themselves on third parties (an evidence chain). Where there is such a chain, the end-user (usually a bank) cannot guarantee that the person, who it relies on, can produce evidence of identity (which it does not hold) without delay, because the person being relied on in turn relies on another etc.

373. The IOMFSA has reviewed current practice by banks in these areas and does not agree with the above findings. It has provided evidence to evaluators to show that the banks concerned are, in fact, operating under, and in full compliance with, paragraph 23 of the AML/CFT Code (i.e. reliance is being placed on eligible introducers). Acknowledging this differing evidence, the extent to which FIs and DNFBPs (and, in particular, banks) may be acting outside the AML/CFT Code is not clear. However, the evaluation team is not in a position to discount the information that was provided during the interviews with the private sector.

---

[41] Under paragraph 23(9) of the AML/CFT Code the FI/DNFBP, when placing reliance on an eligible introducer, must take measures to satisfy itself that the introducer is not itself reliant upon a third party for the evidence of identity of the customer. This is also relevant for para. 374 of the MER.

[42] Under paragraphs 7, 10 and 13 of the AML/CFT Code, there is a legal requirement that the FI/DNFBP must undertake a risk assessment of its customer, and must understand the nature of the customer's business and its beneficial ownership before being able to accept that customer. This is also relevant to para 30, 172, 372, 394, 436 and 503 of the MER.

[43] The "eligible introducer" regime is explained at c.17.1 in the TC annex.

374. In any cases where FIs and DNFBPs do make use of CDD measures applied by non-eligible introducers, they may not: (i) take into account the risk that is presented (or fully mitigate that risk); and (ii) apply the strict safeguards that apply to eligible introductions (which are based on R.17).

375. In cases where FIs explained that reliance had been placed on eligible introducers, it was apparent that: (i) extensive checks were being applied before recognition of a third party as an eligible introducer; and (ii) third party procedures tested periodically thereafter[44]. One large bank went further yet and explained that it also called for all underlying evidence to be provided by the eligible introducer at the start of each relationship with the underlying company or trust, rather than rely on the introducer to hold that evidence (something referred to as a "graduated approach" by the IOMFSA). However, it is possible that reliance might be placed on a third party that is from a country that no longer sufficiently applies the FATF Recommendations because the list of countries that are considered to operate laws equivalent to those of the IoM[45] has not been reviewed for several years (because there have been no recent additions). Recognising this, a review was undertaken by the authorities at the start of 2016 which has highlighted the need to refresh the list.

376. In conclusion, evaluators are of the opinion that the use of CDD information and evidence collected by third parties (including through chains of introduction) increases the risk that CDD measures will not be applied in line with the AML/CFT Code. FIs and DNFBPs may be able to mitigate this risk through terms of business, but evaluators are not in a position to form a view on what is happening in practice and what effect this may have.

Application of risk mitigating measures

377. To mitigate risks, the IoM private sector applies a risk-based approach. As noted above, every institution met on-site described that an overall business risk assessment would be carried out. Additionally, every FI and DNFBP separately assesses customer risk, documents it and reviews it periodically or when a trigger event[46] occurs, within the context of the findings of its business risk assessment. Evaluators were told that, in line with guidance in the AML/CFT Handbook, low risk ratings would not be assigned to a customer and hence no simplified CDD would be applied to any customers or occasional transactions[47]. If, however, a customer would pose a higher risk[48], FIs and DNFBPs would apply enhanced CDD. Indeed, some FIs have even divided higher risk cases into several underlying risk categories, for example into high and significant risk, where more extensive business relationship monitoring and higher level yet of senior management approval would be required for customers presenting a significant risk.

378. Prior to revision of the AML/CFT Code in 2015, some life assurance companies and securities firms did not document their customer risk assessments because they considered that there was no requirement to do so (even though this requirement has been in place since 2008). Additionally, there were some life assurance companies who, other than for higher risk customers, only review customer risk assessments if a trigger event occurs.

379. However, not all online gambling operators apply all elements of a risk-based approach. Online gambling operators explained on-site that they would not apply enhanced CDD when monitoring customer transactions. Instead, comprehensive monitoring systems in place in each operator are

[44] One large bank that provides products and services to TCSPs explained that it now recognised as eligible introducers no more than 15 TCSPs, down from around 40 at its peak, choosing to focus on those with a combination of strongest controls and greatest profit opportunities. A factor in this decision had been its group's risk appetite.

[45] "List C" is a maintained by the Department for Home Affairs.

[46] A significant change in customer profile, occurrence of an unusual transaction etc.

[47] Excluding CDD exemptions that may be applied under paragraphs 20 to 22 and 24 of the AML/CFT Code.

[48] Matters that may pose a higher risk include: (i) activity in a jurisdiction presenting an AML/CFT risk; (ii) connection with a customer resident or located in such a jurisdiction; (iii) use of nominee shareholders or shares in bearer form; (iv) provision of high risk products; and (v) provision of services to HNWIs.

used to monitor transactions for all customers (including higher risk customers) as it was felt that this would be sufficient to detect suspicious activities even for higher risk customers. This raises concerns, not least because the Online Gambling Code states that, if a licence-holder determines that a participant poses a higher ML/TF risk, it must apply enhanced due diligence (including considering what additional on-going monitoring should be carried out), e.g. where there are "red-flags" which merit special attention and monitoring.

380. More generally, the evaluators are concerned about customer risk assessments and ultimately enhanced CDD application for higher risk customers in the IoM. It is very common that FIs and DNFBPs do not see the beneficial owner face-to-face and, on the contrary, use third party introducers extensively (e.g. TCSPs, law firms, etc.). Whilst permitted under the standards, such a business model increases inherent risk. Additionally, many customers are non-resident without any IoM connection, HNWIs or have high profile beneficial owners wishing to structure their assets in a tax efficient manner – factors given as examples of potentially higher-risk situations in the interpretative note to R.10. However, the percentages of customers assessed by some (but not all) FIs and DNFBPs as presenting a higher risk appear low[49], compared to the risks that are present in the IoM. In addition, it is felt that TCSPs downplay risks in their sector. Evaluators are concerned that enhanced CDD measures, including monitoring, will not be applied where customers that actually present higher ML/TF risk are not rated accordingly, although it is recognised that the AML/CFT framework in place for insurers requires all insurers to obtain source of wealth as standard reflecting the higher inherent risk present in this sector. In response, the IOMFSA has said that numbers of customers assessed as presenting a higher risk have not generally been lower than expected.

Application of CDD and record keeping requirements

(a) CDD

381. Beneficial ownership requirements in the AML/CFT Code are generally well understood and all FIs and DNFBPs interviewed confirmed that they would request information leading to the ultimate natural person behind the customer. Representatives of sectors seemed aware of the characteristics of legal arrangements and their use in corporate structures. The majority of representatives met said that they would consider the source of wealth for a business relationship in order to satisfy themselves that they have found out the real beneficial owner of a legal person or legal arrangement. However, due to the fact that the markets are internationally focused, with business originating from over 190 countries, the availability of beneficial ownership information, the reliability of the identification infrastructure and the availability of independent information sources will ordinarily vary according to the jurisdiction of residence of the customer (or beneficial owner).

382. Given the use of complex ownership structures, guidance is provided in the AML/CFT Handbook on information that could be obtained in order to meet the requirement in the AML/CFT Code to understand the ownership and control structure of a customer. This may include structure charts and lists. Guidance is also provided in the AML/CFT Handbook on which natural persons will be considered to ultimately own or control a trust arrangement, who might be considered to be a controlling party (other than the trustee) and also the risk of use of dummy settlors. The sector specific section for TCSPs also explains what is meant by the term "known beneficiary". However,

[49] This can be illustrated by three examples taken from a number of responses provided by the private sector. One bank interviewed said that around 7% of its customer base presented a higher risk notwithstanding the higher risk target markets that it had described. A law firm that had explained that complex structures were common advised that 2% of "matters" were considered to present a higher risk. And one life assurance company explained that less than 1% of its customer base was considered to present a higher risk notwithstanding that most business was sourced from other international finance centres and its target market included high net worth individuals.

guidance does not consider ways in which individuals may control a structure through indirect holdings nor clarify the requirements that apply when a settlor, beneficiary etc. is not an individual.

383. One bank said that it would request a copy of the trust document (or equivalent) and letter of wishes (or similar) when establishing a business relationship with the trustee. Other banks do not. A number of TCSPs met said that they would be happy to provide such documents if requested to do so. Evaluators consider that, in certain cases, failure to review such documents increases the risk that the person who exercises ultimate effective control over the trust may not be found out.

384. When asking about the purpose and intended nature of a business relationship, FIs and DNFBPs usually ask why the customer wishes to establish the business relationship and how the account will be operated (including transaction volumes). For corporate customers, information would also be asked about business partners and sometimes information about the customer's knowledge of operating in given fields. In the case of securities firms and life assurance companies (providing unit-linked products), questions are asked to understand the customer's investment appetite and needs, the latter having also several key information fields that will help the FI to understand the business relationship for CDD purposes. The majority also suggested that information about source of wealth would be requested from every customer and the extent of corroboration of that information would depend on the customer's risk profile and services offered. Notwithstanding the importance of such corroboration (e.g. to mitigate the elevated risks stemming from a combination of non-face to face and non-resident customer relationships), the AML/CFT Handbook does not explain what measure might be applied.

385. While in most cases FIs and DNFBPs know what CDD must be applied, there are some examples of failings in the application of CDD measures, particularly for TCSPs[50] that are relied on by banks and securities firms when commencing a business relationship. Currently, the police are investigating a TCSP found to have materially breached AML/CFT Code requirements, including requirements to identify and verify the identity of the ultimate beneficial owner of customers[51]. Additionally, from 37 visits conducted of TCSPs in 2015 (sampling 370 CDD files), the IOMFSA found that CDD was not properly undertaken in: (i) six files during business commencement (including one high impact[52] and one medium impact[53] TCSP); and (ii) four files during the course of a continuing business relationship (including one high and two medium impact TCSPs). Additionally, four files sampled had shortcomings, two of which are material, with regard to beneficial owner identification and verification (including two medium impact TCSPs). Deficiencies were found in the application by TCSPs of eligible introducer provisions (reliance on third party) on three files (one of which relates to a high impact TCSP). Similar findings in similar quantity have also been detected in 2013 and 2014.

386. When using CDD information and evidence provided by eligible or non-eligible introducers, banks and other parties are exposed to any weaknesses that arise in CDD conducted by the introducer and so weaknesses identified earlier about "information chains" are also relevant here.

(b) Enhanced CDD

387. In all higher risk cases, FIs and DNFBPs would apply enhanced CDD (except as noted earlier for some online gambling operators). It was explained that FIs and DNFBPs would gather more information to verify the customer's and beneficial owner's identity, and take more measures to

[50] It should be noted that the IoM has signed up to both FATCA and the OECD Common Reporting Standards placing a further requirement upon TCSPs to maintain and provide accurate BO information.

[51] Breaches were found in requirements in place at the time covering risk assessment, identification procedures, new business procedures, on-going monitoring, PEPs and staff training.

[52] A TCSP has a high impact where it: (i) has 50 or more staff; or (ii) administers 1,400 or more companies and trusts.

[53] A TCSP has a medium impact where it: (i) has between 10 and 49 staff; (ii) provides corporate services to a company with listed securities or which is admitted to trade on a stock exchange; or (iii) administers more than 500 but less than 1,400 companies and trusts.

understand the intended nature and purpose of the business relationship. FIs and DNFBPs would also ask for more information about source of wealth, when on-boarding a customer, and source of funds, during the customer relationship, and would, in addition to automated monitoring systems, have manual annual checks to establish whether the whole customer picture (not every transaction separately) corresponds to what is expected.

388. However, during interviews with evaluators, a number of FIs and DNFBPs (three life assurance companies, one TCSP and one online gambling operator) could not explain what more is actually done when higher risk customers are involved, describing the same set of measures that would be done for every customer. It is considered that this reflects the lack of guidance on the matter in the AML/CFT Handbook and the Online Gambling 2015 AML Guidance which do not explain what the additional steps to be taken could be. This is contrast to section 1.4 of the IGN (other enforceable means) which specifies the type of measures that must be applied by life assurance companies. The IOMFSA's themed visit programme (2012 to 2013) had identified the same issue in some banks and had also found a number of cases (since remediated) where a customer had been assessed as presenting higher risk but where there was no evidence that enhanced CDD had been applied in practice.

(c) On-going due diligence

389. Most FIs and DNFBPs met on-site described the automated transaction monitoring systems that they have in place. These systems will automatically search and report any unusual patterns of transactions. Reports (or alerts as one may call them) will then be independently reviewed to ensure they are in line with the knowledge of the customer. Separately, manual monitoring can be done (or for smaller FIs and DNFBPs only this kind of monitoring will be done), whereby customer managers or other staff members consider whether transactions made, or orders placed, by customers are in line with information collected during business establishment. The NRA notes that monitoring is less formalised than might be appropriate in the securities sector. This reflects the smaller size of some securities firms.

390. As for customer screening, the majority of FIs and DNFBPs use commercial databases (such as World-Check, Dow Jones etc.) to identify any connection to a PEP, any adverse media information about the customer, or any possible connection to any sanctions designation before account take on and thereafter on an on-going basis. On the other hand, the IOMFSA's themed visit programme (2012 to 2015) found that banks had, in some cases, failed to record all parties on their systems (e.g. directors, shareholders, beneficiaries etc.) ultimately preventing all parties being screened appropriately on an on-going basis (sweeps of systems). In cases where screening is not automated (for example, some TCSPs, some law firms, some smaller securities firms and some life assurance companies), FIs and DNFBPs met said that customer information will be screened at least during the customer take-on process and when any trigger event happens or CDD is being updated.

391. Regular reviews of CDD are also undertaken by FIs and DNFBPs, with all higher risk customers being reviewed at least on an annual basis. Sometimes PEP relationships will be reviewed more frequently, especially by banks. For standard risk customers, reviews and CDD updates are usually done every three years. The review will encompass an examination of the CDD held for the customer, together with a review of transactions to see if these are in line with FI or DNFBP expectations.

392. In addition to regular reviews, customer files would be reviewed when trigger events occur, e.g. a significant change in a customer profile. FIs and DNFBPs met during the on-site visit also declared that CDD measures would be re-applied if an unusual transaction occurred or if there were doubts about the veracity or adequacy of previously obtained customer identification data.

393. However, some FIs (including life assurance companies and securities firms) and DNFBPs explained that they sometimes rely only on trigger events (such as the investment of additional money, payment of premiums or positive screening "hit") to update CDD information. As a result, CDD information may not be updated for several years, which affects the understanding of a business

relationship. Several changes to a customer's profile could be missed that would affect the level of monitoring and understanding of the customer, particularly if there are also weak screening systems. Evaluators are of the opinion that reliance on trigger events to update CDD information is not in line with c.10.7. A case highlighted in one interview shows the importance of periodic reviews of CDD information. Such a review had highlighted that a customer of a TCSP had been sentenced to prison for securities fraud, something that would not have been identified if the customer's file had not been updated.

394. While FIs and DNFBPs may have generally demonstrated knowledge, and may be aware of monitoring and screening duties, weaknesses identified earlier about "information chains", where incomplete or false information may be provided through a chain of third parties, may also be relevant here. Additionally, application of on-going due diligence may also be limited where there are failings in the application of CDD measures by third parties, e.g. those highlighted for TCSPs.

395. In line with requirements in the AML/CFT Code, the evaluators were told that no business relationship would be commenced if the level of CDD collected is unsatisfactory, if there are any doubts about the veracity of the obtained information, or if there is ML/TF suspicion. Similarly, if, during a business relationship, FIs and DNFBPs had doubts about the veracity or adequacy of previously obtained customer identification information and could not re-apply CDD, or if a ML/TF suspicion could not be discounted, the business relationship would be terminated. The evaluators spoke to two businesses (one life assurance company and one TCSP) that, contrary to the AML/CFT Code, said they would not terminate a business relationship pursuant to c.10.19(a) if that FI has applied CDD because of ML/TF suspicion (c.10.2(d)) but still could not overcome that suspicion (because of insufficient CDD information). The evaluators also identified a case where a securities firm had not applied CDD while having ML/TF suspicion, but instead had turned to the third party that it had placed reliance on (a TCSP) and asked the TCSP: (i) to confirm that CDD had been applied properly; and (ii) what it thought about the securities firm's suspicion. The latter remark suggests that not all FIs are familiar with the duty to apply CDD in the case of suspicion or the risk of tipping-off suspected customers (in this case through the TCSP) where enquires are not appropriately handled.

(d) Record-keeping

396. Records, such as CDD documents, account files and business correspondence will be held at least for five years following the termination of the business relationship. Records with the results of any analysis undertaken on CDD measures or account files would also be kept in the same manner. All transactions records will also be kept for a minimum of five years, but following the completion of the transaction. However, if a STR is made about a customer, all FIs and DNFBPs interviewed explained that CDD documents, account files, business correspondence, transaction information and any analysis undertaken would be kept indefinitely.

397. All FIs and DNFBPs also confirmed that records are kept (in archives or digitally) in a way that they could be swiftly disseminated to competent authorities upon request under statutory provisions.

Application of EDD measures

(a) PEPs

398. Most FIs and DNFBPs use commercial databases to identify domestic and foreign PEPs, prominent function holders in international organisations, and family members and close associates of such persons. While some FIs and DNFBPs use an application form to ask the customer to indicate whether they are a PEP (or connected to a PEP) and to provide information on occupation, the practice was not universal. In those cases where the FI or DNFBP does not ask the prospective customer whether he is a PEP and/or occupation as part of account opening formalities, there is a potential risk that the customer may not be identified as a PEP. Moreover, there were some on-line

gambling operators with significant numbers of customers that did not: (i) apply additional measures to understand whether their customer was a PEP, family member, or close associate, e.g. request information on status or occupation; or (ii) regularly screen customers against commercial databases.

399. In the case of all PEPs, family members and close associates identified, FIs and DNFBPs would assign high risk ratings to those customers. Additionally, senior management would approve all such customer relationships. While the majority of FIs and DNFBPs interviewed explained that information about source of wealth and source of funds would be asked for every customer, it would be done always and more thoroughly when a PEP is involved. In these cases, the level of information that would satisfy FIs and DNFBPs would be higher. Customer relationship monitoring would also apply lower thresholds to transactions and additional parameters would be used to ascertain unusual transactions.

(b) Correspondent banking

400. Cross-border correspondent banking and other similar relationships are not offered by FIs in the IoM.

(c) New technologies

401. ML/TF risks are assessed when developing new products and new business practices, including new delivery mechanisms, and when using new or developing technologies for both new and pre-existing customers. This assessment would be covered in the business risk assessment done and reviewed annually by every FI and DNFBP met on site, or through a separate technological development risk assessment (in line with requirements in the AML/CFT Code).

402. Some FIs and DNFBPs met on-site provide only very limited services and had no intention to widen the scope of their activities or delivery channels. Accordingly, they did not address these matters in a risk assessment.

(d) Wire transfer rules

403. In line with legislation in effect in the EU, the AML/CFT Code currently requires FIs to obtain information on the originator of a wire transfer but not also the beneficiary. This will be remedied when the EU legislation is updated. Nevertheless, banks met explained that their information systems already require all information on both beneficiaries and originators to be included with the transfer and that the transfer would be rejected if this information was missing.

404. Evaluators were also advised that, where banks operate as a beneficiary or intermediary financial institution, they have rules in place on how to proceed if obligatory information is missing, i.e. whether to execute, reject or suspend a wire transfer. Given the legislative shortcoming, however, it is not possible to firmly state that all FIs would take measures should beneficiary information be missing.

(e) Targeted financial sanctions relating to TF

405. Effectiveness issues connected to targeted financial sanctions are considered in detail under IOs 10 and 11. These include: (i) the mechanism used to communicate designations to FIs and DNFBPs; (ii) detection of funds, or other assets, that are jointly owned or controlled, directly or indirectly, by designated persons or entities; (iii) effectiveness issues identified under IO 4 and understanding of the private sector; and (iv) steps to be taken should assets held by complex structures be detected.

(f) Higher risk countries identified by the FATF

406. The majority of FIs and DNFBPs met advised that they would not accept (or continue) business relationships with customers (or beneficial owners thereof) connected to countries on lists published by the FATF as having weak AML/CFT requirements.

407. Those that would accept or continue such relationships would apply enhanced CDD.

Reporting obligations and tipping off

408. As indicated in the IoM's NRA and acknowledged by a number of authorities, the rather low quality of SARs throughout all sectors is of concern. The FIU advised evaluators that just 25-30% of all reported SARs actually contain suspicion of ML/TF and/or underlying criminality. Most SARs are filed by banks. (see Table 2 on the number of SARs). Whilst some DNFBP sub-sectors have increased their activity in terms of SAR reporting, the FIU suggested that most are not relevant for its work and, at times, merely highlight links to potential ML/TF indicators, such as use of tax optimisation schemes.

409. Although the authorities identified quality of reporting as an issue some time ago and have taken steps to bring about improvement in this area (e.g. by informing reporting entities on an individual basis and through the annual AML/CFT conference organised by the IOMFSA) the situation has not improved significantly in recent years. Evaluators believe that there are a number of reasons for this.

410. A large majority of private sector representatives met on-site appear to focus on the protection that may be given by an "authorised disclosure", a means by which a defence against ML or TF can be obtained through seeking consent from the FIU to commit a prohibited act. Hence, many FIs and DNFBPs, suggested that they would tend to make a report without carrying out additional research in order to confirm that there is credible suspicion, e.g. where there is use of tax optimisation schemes. Evaluators consider that this is indicative of defensive reporting and has the effect of clogging up the system with low quality information.

411. In contrast, some other reporting entities met on-site, including some large banks and TCSPs, appear to apply a high test when considering whether the particular circumstances of a case provide reasonable grounds for knowing or suspecting ML/TF. They would require clear and definitive confirmation of a suspicion before making a SAR. As no sanctions have been imposed for failing to report or late reporting during the period under review, there is no additional incentive for FIs and DNFBPs to change their behaviour and perception vis-à-vis reporting SARs.

412. During interviews, many private sector representatives, including those representing institutions which have a significant portion of the market share, appeared not to properly understand the reporting requirement. Many responded in the negative when presented with scenarios which would normally trigger the submission of a SAR.

413. Some categories of DNFBPs suggested that the FIU often encourages reporting entities to report all situations, even those which only give rise to unusual conduct. In addition, all private sector representatives met on-site expressed the need for more precise and case-by-case feedback rather than a generic response sent to all reporting entities upon reporting. Latterly the FIU function of the FCU, and thereafter the newly established FIU recognised its role within the overall AML/CFT regime as a filter between private sector and law enforcement and expressed the need to hold talks with professional associations and certain reporting entities (e.g. those that report the most or the least), depending on current trends, methods and typologies, on a more frequent basis, i.e. quarterly. This practice would also allow the FIU to provide more specific feedback to each sector and also on an individual basis.

414. Mention is also made under IO 6 of reporting by call centre operations where the business relationship or one-off transaction has no specific connection to the IoM.

415. In prescribed circumstances, POCA 2008 permits FIUs and DNFBPs to disclose to a third party that a SAR has been made to the FIU. In practice, these provisions appear to be used carefully. However, one case referred to above under on-going due diligence emphasises the importance in

appropriately handling cases where information has been provided by an introducer (particularly those where there are chains).

416. Operational issues and implications with regard to reporting are discussed under the relevant paragraphs under I.O. 6, including the need for more precise and case-by-case feedback to be provided on SARs.

Internal controls and legal/regulatory requirements impending implementation

417. Many FIs and DNFBPs (including TCSPs) met onsite apply three-lines of risk management: (i) daily business controls; (ii) compliance and risk oversight; and (iii) internal and external audit. Many of the banks and life assurance companies met on-site are parts of larger groups and so will be covered by a group-wide internal audit function. Internal audits of AML/CFT issues would usually be performed annually or every two years depending on the audit plan.

418. Whilst there is a requirement in the AML/CFT Code for all FIs and DNFBPs to maintain appropriate procedures for monitoring and testing compliance, there is no specific AML/CFT Code requirement to have an independent audit function. However, there are relevant rules in the FSRB requiring most FIs and also TCSPs to establish and maintain comprehensive policies appropriate to the nature and scale of their business, including independent internal audit and compliance procedures to test compliance with regulatory requirements, and certain FIs have to have an internal audit function. The IA 2008 also contains relevant requirements.

419. Accordingly, some FIs and DNFBPs that are not also regulated under the FSA 2008 or IA 2008 have not established such a function. Moreover, there were also cases in some sectors (such as insurance and some online gambling operators), where the evaluators were told that, although internal control systems were in place, internal audit scope would not cover AML/CFT issues, and some securities firms had not established internal audit functions. It is also relevant that FIs and DNFBPs are not required to appoint a compliance officer under the AML/CFT Code (though such an appointment is mandated for those FIs and DNFBPs regulated and supervised under the FSA 2008 and insurance companies must establish a compliance function).

420. There are no legal or regulatory requirements (e.g. financial secrecy) impeding the implementation of internal controls and procedures. Indeed, in cases where FIs or DNFPBs are part of a larger group, group policies would also be applied. However, if the IoM law has higher standards in any part compared to a jurisdiction where the group operates, those higher IoM standards would be applied.

Conclusion

421. **The IoM has achieved a Moderate level of effectiveness for IO.4.**

CHAPTER 6. SUPERVISION

Key Findings and Recommended Actions

Key Findings

• The supervisory actions in all fields are effective in preventing criminals and their associates from being directors and beneficial owners of FIs, TCSPs, casinos and online gambling operators. With regard to other DNFBPs, effectiveness could not be fully demonstrated since registration of DNFBPs under the DBRO Act was still on-going.

• The IOMFSA does not routinely collect statistics and information that allow it to fully consider ML/TF risk in the financial sector as a whole and at sector level; this includes information on the extent to which FIs and DNFBPs utilise concessions, including the use of introducers.

• AML/CFT risk is considered for each institution. Based on this assessment, the IOMFSA records those FIs and TCSPs that are to be treated as presenting a higher risk – irrespective of that entity's average risk score (taking factors other than ML/TF into account). However, the IOMFSA was not able to provide a snap-shot of the ML/TF risk profile of all FIs and TCSPs. Accordingly, it is not clear how it considers sectorial risk and whether overall ML/TF risk rating spreads are consistent with sectorial analyses of risk in the NRA.

• IO 4 notes that banks may use CDD information presented by TCSPs that have collected this information in turn from other parties. IO 4 also highlights an on-going enforcement case that has shown that, for many customers, the TCSP (which banks in the IoM) did not hold on its files information required under the AML/CFT Code. Accordingly, there is an increased inherent risk that a bank may be provided with incomplete or false information and not able to understand the nature of the customer's business and its ownership or control structure. This has a spill-over effect on banks, that use TCSPs to provide CDD information, which has not received sufficient attention by the IOMFSA.

• Whilst the absence of specific statistics on numbers and results of AML/CFT visits conducted by predecessors of the IOMFSA before 2015 has an impact on assessment of effectiveness in this area, results of themed visit programmes (banking and life assurance) and inspections of TCSPs between 2013 and 2015 point to an active supervisory approach.

• The DNFBP supervisory and enforcement section in general at the IOMFSA is understaffed for the purposes of supervising such a diverse sector.

• There has been over-reliance in the past by the IOMFSA on the use of remediation plans to address AML/CFT deficiencies; nonetheless the supervisor has already taken steps to address this issue.

• While the GSC has supervised AML/CFT since 2011, this has until recently been on the basis of a rolling programme. Only recently has the GSC completed the work necessary to implement a risk-based approach. This means that it is not possible to assess its effectiveness at this time. Supervision of some FIs and DNFBPs under the DBRO Act started only at the beginning of 2016 (though members of the Law Society of the IoM and some accountants have been supervised since 2011). These gaps in supervision have an impact on the degree to which this IO has been met. Had current oversight arrangements been in place for the whole of the evaluated period, these would have been seen as effective.

• The maximum penalty that may be applied to lawyers and accountants under the DBRO Act is GBP 1 000 and it is not effective at ensuring future compliance by sanctioned entities or dissuasive of non-compliance by others.

• The GSC is unable to apply a full suite of effective, proportionate and dissuasive sanctions. It is able only to revoke a licence of an online gambling operator or to direct that a director or other person exercising managerial functions be removed from their position or deprived of their function.

Recommended Actions

• In accordance with findings of the NRA, the IOMFSA should collect statistics and information that will allow it to better consider ML/TF risk in the financial sector as a whole and at sector level; this includes information on the extent to which firms utilise concessions, e.g. use of introducers. In turn, statistics and information collected should be used to enhance the IOMFSA's supervision of sectors, most notably TCSPs and banks, where the use of introducers and intermediaries is identified as an inherent risk.

- More staff should be available for supervision of entities under the DBRO Act and enforcement in the IOMFSA.
- As identified in the NRA, additional supervisory and sanctioning powers should be given to the GSC.
- The IOMFSA should, in severe cases, make greater use of sanctions.
- Gaps in the scope of regulation and supervision of FIs and DNFBPs identified at c.26.1 and c.28.2 should be addressed.

The relevant Immediate Outcome considered and assessed in this chapter is IO3. The recommendations relevant for the assessment of effectiveness under this section are R26-28 & R.34 & 35.

Immediate Outcome 3 (Supervision)

422. The IOMFSA is now the supervisor for all FIs and DNFBPs[54] (except online gambling and casinos). It is worthy of note that TCSPs are regulated and supervised in the IoM like financial institutions. After considering risks, the authorities have decided to include more entities in both categories than are covered under the FATF Recommendations. Therefore, the IOMFSA supervises for AML/CFT purposes also captive insurance companies, and institutions like payroll agents and virtual currency operators.

423. Up until October 2015, the Law Society of the IoM ("Law Society") and five UK accountancy bodies (including the Institute of Chartered Accountants in England and Wales ("ICAEW") and Association of Chartered Certified Accountants ("ACCA")) had responsibility for monitoring compliance by their members in the IoM with the AML/CFT Code under memoranda of understanding in place with the DHA.

424. Under arrangements now in place with the IOMFSA, the Law Society and UK accountancy bodies can continue to supervise their members under the Designated Business (Registration and Oversight) Act 2015 ("DBRO Act") as agents for the IOMFSA. Evaluators understand that most lawyers and around 40% of accountants (that are regulated for audit purposes by UK professional bodies) have elected to be supervised by their professional body – under supervisory arrangements set and overseen by the IOMFSA. Responsibility for enforcement measures will rest with the IOMFSA.

425. The new oversight model has a number of advantages. Whereas the Law Society and UK accountancy bodies may continue to supervise their members, there will be much better coordination of supervision across sectors and specific sanctions in place under the DBRO Act to punish failure to comply with AML/CFT requirements. And for accountants, the supervisory model to be applied will be bespoke to the IoM, and improve accountability of the UK accountancy bodies. Under the new oversight model: (i) visits will be conducted in accordance with IOMFSA guidance: (ii) findings will be reported to the IOMFSA; (iii) joint visits will be conducted; and (iv) working papers will be available to the IOMFSA on request.

426. Terrestrial and online gambling activities are regulated and supervised by the GSC.

Licensing, registration and controls preventing criminals and associates from entering the market

427. The IOMFSA and the GSC both have powers to prevent criminals and their associates from entering the market and being the beneficial owners or directors of supervised entities. The evaluation team was advised about cases in which the IOMFSA had prevented both legal and natural

[54] As noted in the TC annex, not all FI activities are regulated or supervised. As also noted in the annex, acting as a partner by way of business is not considered to be regulated and supervised.

persons from entering or continuing in the market (the latter group through disqualification procedures or giving notice to an employer or prospective employer of activities or circumstances prejudicial to an individual's fitness and propriety under regulatory legislation). The IOMFSA advised that it had received 32 applications from legal persons under the Financial Services Act 2008 between 2013 and 2015, of which nine had been discouraged from pursuing licensing due to AML/CFT concerns and withdrawn their applications (so that it was not necessary to use statutory powers). As far as natural persons are concerned, those cases related to prudential issues (rather than concerns about criminality). The evaluation team was provided with a list of cases illustrating effectiveness in this matter.

428. The registration process for a number of DNFBPs and FIs under the DBRO Act, which started in October 2015, was still on-going during the on-site visit[55]; therefore there is a risk that some of those institutions may be controlled by criminals and/or their associates. This risk however will be mitigated as applicants are registered[56].

429. In relation to online gambling the GSC also has a track record of turning down applications where it is concerned that the applicant will not comply with laws and regulations; there have been three since 2009. The GSC is required to have regard for "integrity" in its licensing decisions.

430. At the request of the IOMFSA, the court has successfully disqualified persons (company officers) in 12 cases from holding corporate office (in the IoM and elsewhere) since 2008 (the most recent of which was in 2011), where in some instances previous criminal charges have been present. Other cases are currently pending. This sanction is considered when there has been general corporate misconduct and disqualification is not limited to regulated activities.

431. The evaluation team has established that the IOMFSA "patrols its perimeter" in order to establish whether there are institutions which should be licensed or registered, but have failed to do so. This is of particular importance as, during the on-site visit, the IOMFSA was in the process of registering DNFBPs and FIs under the DBRO Act, as they have taken on, or over, responsibility for AML/CFT supervision in this respect.

Supervisors' understanding and identification of ML/TF risks

432. As an international financial centre, the IoM's financial system is particularly vulnerable to ML, which supervisors recognise. Given the international nature of its business model, there is a risk that its products and services (including legal persons and legal arrangements) may also be used to finance terrorism.

IOMFSA

433. The general ML/TF risks in the financial (and other sectors) are understood by the IOMFSA, including additional sectors such as pensions and captive insurance that are supervised for AML/CFT compliance in the IoM (which seems adequate from the perspective of the centre's activities). This understanding is facilitated by long-standing and thorough supervision (including on-site visit programme and access to SARs) over most of the sectors.

434. However, the NRA has highlighted that there are gaps in statistics and information that are available to the authorities. For example, the IOMFSA does not routinely collect and aggregate information across all sectors on customer risk classifications, numbers of PEPs, residence of beneficial owners of customers, or extent to which exemptions or simplified CDD measures are applied under the AML/CFT Code (deficiencies highlighted under IO1)[57]. And, whereas the NRA considers and assesses the ML/TF risk of each financial sector, the IOMFSA did not identify and

[55] The IOMFSA expected to have registered all applicants by the end of August 2016.
[56] During the registration process, the IOMFSA identified a DNFBP controlled by a convicted criminal. This application was refused.
[57] The IOMFSA does collect some information of this nature as part of AML/CFT visits.

maintain an understanding of the ML/TF risk between different sectors and type of institution, or allocate resources based on such an understanding.[58] Instead, its focus is on risk assessments of individual FIs and DNFBPs. One effect of this may be a less optimal use of the IOMFSA's resources.

435. AML/CFT risk is considered for each institution. Based on this assessment, the IOMFSA records those groups and licence-holders that are to be treated as presenting a higher ML/FT risk – irrespective of that entity's average risk score (taking factors other than ML/TF into account). The IOMFSA was able to explain what percentages of life assurance companies present a high risk (approximately one third), medium risk or low risk of ML/TF. However, it was not able to provide a snap-shot of the ML/TF risk profile of all FIs. This is because the IOMFSA's risk model reflects other risks in its risk matrix (consistent with its function as a supervisor of prudential and conduct of business matters). Accordingly, it is not clear how it considers whether overall ML/TF risk rating spreads are consistent with sectorial analyses of risk in the NRA.

436. IO 4 explains that some FIs (particularly banks) may use CDD information presented by a third party (especially TCSPs) that has collected this information in turn from another party, for example, from a local or overseas law firm. Accordingly, there is an increased inherent risk that a bank may be provided with incomplete or false information and not able to understand the nature of the customer's business and its ownership or control structure. IO 4 also highlights an on-going enforcement case that has shown that, for many customers, the TCSP (which banks in the IoM) did not hold on its files information required under the AML/CFT Code, including beneficial owner information.

437. In discussions with the IOMFSA, it became apparent that the regulator was not fully aware of the possible "spill-over" effect between banks and TCSPs, even though the on-going case referred to might have been expected to prompt consideration of the knock-on effect on the bank that had made use of the TCSP. It seems that a better flow of information between divisions at the IOMFSA (especially prudential – enforcement) would have facilitated a better understanding of said issues, and possibly further supervisory action[59].

438. The extent to which use is made of eligible introducers to verify identity across the banking and other sectors is also not considered sufficiently by the IOMFSA (at an aggregated level). Whilst the use of introducers was covered in the NRA and the IOMFSA does consider such matters (directly or indirectly) in entity risk assessments and on-site examinations, the IOMFSA does not hold aggregated statistical data regarding who is using eligible introduction provisions, which TCSPs and other intermediaries are being used, or in which countries eligible introducers are resident.

439. In the case of relationships between TCSPs and banks, there is also the problem of ML/TF risk concentration, as one of the banks has relationships with one third of TCSPs in the IoM. Whilst this risk could be mitigated by the application of extensive checks on TCSPs, the IOMFSA did not appear to have considered the disruption that could follow a systemic failure in the bank's application of AML/CFT requirements.

440. Despite promoting development of the use of virtual currencies, the jurisdiction had yet to consider risks that are inherent in such currencies at the time of the on-site visit. It was explained that risk could only be properly assessed when the IOMFSA's registration process is finished. The NRA and the IOMFSA recognise the need to carry out further work on virtual currency operators.

[58] Since the on-site visit, the IOMFSA has started to produce overview documents for each sector that provide a sector overview, identify trends, macro developments, risks and threats (in order of priority), identify supervisory risks, and consider resourcing, supervisory tools, and characteristics of FIs and groups (including diversity and number). Documents address ML/TF risk. The IOMFSA has explained that these overview documents will be presented to the Board.

[59] This is something that has already been recognised by the IOMFSA, which has finalised and re-focussed the mandate of its remediation panel and made changes to processes.

GSC

441. The GSC now has a good understanding of the ML/TF risks facing the gambling sector. This was not the case before the NRA - which highlighted that the GSC did not capture the statistical data necessary to make definitive statements about sector risk. The GSC is now in a position to recalculate its NRA scores in real time, and the scores incorporate ratings from its latest AML/CFT inspections.

442. Risks identified are now also being fed into the regulator's "risk-ladder" - a complex in-house data gathering tool - which scores each licence-holder. This tool, along with the on-going on-site visit process (findings, which are analysed and compared to previous visits and between supervised entities) feeds into the supervisor's understanding of the risk and specificities of the sector. Unfortunately, whilst work on the introduction of a risk-based approach to supervision had started in May 2015, use of the tool had just been introduced by the GSC a week prior to the on-site visit, which was still building a visit approach based on the information identified. The GSC has explained that it takes about a year to build the appropriate infrastructure.

443. More generally, the GSC is also looking to invest in systems to better analyse the vast amounts of data that it collects. A project to commission a bespoke regulatory platform[60] started in 2015, and this platform will eventually replace the in-house tool.

444. Whilst ML/TF risk was not fully understood by the supervisor until recently, there is considerable overlap with action needed to prevent cheating, collusion and fraud (where gambling is against the house) and online gambling operators have a vested interest in examining requests for withdrawal of money. Accordingly, Manx law limits the use of cash for on-line gambling and requires that winnings are repaid to the original instrument used to deposit funds or to an instrument that the operator is satisfied will result in the customer exclusively receiving the withdrawal.

Lawyers and accountants

445. The Law Society has used a risk-based approach to supervising advocates, and it is the evaluation team's opinion that it understands the inherent risks in its supervised sector (based mostly on outcomes of on-going supervision and cases), e.g. in relation to the potential abuse of pooled client accounts operated by law firms which was considered as part of onsite examinations in 2011/12.

446. Evaluators did not meet with supervisory staff from any of the UK accountancy bodies, and supervision appears to be based on risks present in the UK rather than in the IoM. However, activities conducted in the IoM (and consequently risks) are very limited. In particular, advice on how to establish corporate structures is not given by Manx accountants and few operate client accounts.

Risk-based supervision of compliance with AML/CTF requirements

IOMFSA

447. The IOMFSA applies a risk-based approach to supervision based on a "supervisory approach" document issued in April 2011 and published on its website. This document covers activities that are supervised for prudential and conduct of business purposes under the FSA 2008, so excludes life assurance and includes TCSPs. Whilst the IOMFSA has not outlined its basis for supervising life assurance companies in a similar document, it also applies a risk-based supervisory programme.

448. In line with its supervisory approach, the IOMFSA assigns risk ratings to institutions, and those ratings provide the basis for further supervisory actions, such as on-site visits. Inter alia, the risk rating and risk profiles of particular institutions are influenced by the off-site collection of data and results of supervisory on-site visits. A variety of other factors is also taken into consideration in

[60] This development of a bespoke regulatory platform is a joint project between the IOMFSA and the GSC with the benefits of enhanced analysis expected to accrue to both supervisors.

assessing risk, including (but not limited to): AML knowledge of staff, availability and access to beneficial ownership information, effectiveness of compliance systems, customer type assessments, etc.

449. The IOMFSA has explained that "prudential distortion" (i.e. insufficient focus on FIs and TCSPs that present a lower prudential risk but higher ML/TF risk) is not an issue in practice and would not cloud the IOMFSA's judgement on ML/FT risk and actions for individual institutions. In practice, where ML/TF risk is assessed as high, there is a suitable supervisory response (irrespective of the IOMFSA's assessment of other risks). The supervisor presented evaluators with a list of 24 groups and licence holders regulated under the FSA 2008 that had been assessed as presenting a higher risk due (or partly due) to ML/TF reasons. Nevertheless, neither the "supervisory approach" document nor other IOMFSA methodology or guidance address the possibility that ML/TF risk may be "averaged" with other risks that are taken into account, such as financial failure and misconduct and mismanagement. Nor does the risk scoring matrix used for the assessment of inherent risks presented by TCSPs to the IOMFSA's core objectives separately record ML/TF risk, although the IOMFSA's core supervisory objectives (which include incidence of ML/TF) must be considered when applying a score.

450. Following completion of the NRA, the IOMFSA is to refine its regulatory risk assessment of ML/TF risks for banks, and is considering use of a stand-alone ML/TF risk assessment – based on the World Bank NRA tool. Accordingly, a new AML/CFT risk assessment template and guide has been prepared and is being piloted for three banks.

451. Supervision of a number of DNFBPs and FIs under the DBRO Act by the IOMFSA is very recent, so effectiveness could not be demonstrated. The IOMFSA's supervisory approach is set out in detailed procedures (last updated in December 2015). The registration process had barely finished at the time of the on-site visit, and only a few supervisory visits had taken place.

452. Whereas supervisory staff at the IOMFSA are knowledgeable, and clearly understand their responsibilities and powers, as confirmed by market participants during interviews with evaluators, the DNFBP supervisory section at the IOMFSA is understaffed for the purposes of supervising such a diverse sector. Currently the team is led by one manager, with two assistant managers and an administration officer in the team, although one part-time manager in the AML unit (policy) could be called upon to provide assistance in some cases. The supervisory section has direct supervisory responsibility for over 200 FIs and DNFBPs, including lenders, virtual currency operators, estate agents, SPNOs, and some lawyers and accountants. In addition, it also has responsibility for oversight of supervisory arrangements in place between the IOMFSA and: (i) the Law Society of the IoM; and (ii) UK professional accountancy bodies, e.g. the Institute of Chartered Accountants in England and Wales.

453. The following table provides information on the number of AML/CFT onsite examinations conducted by the IOMFSA in the period from 1 March 2014 to 28 February 2015 (except where indicated), the first full year that information of this type was collected (except for life insurance).

Table 12

Sector	Registered	Total number of on-site visits	Number of AML/CFT specific on-site visits	Number of combined on-site visits (AML/CFT and general)
Banks	26	13	11	1
Funds and investment services	88	43	4	34
Life assurance (2015 calendar year)	15	13	13	0
MSBs and exchange offices	6	3	2	1
Trust and company services providers	177	55	7	46

454. Evaluators were provided also with findings from two themed visit programmes conducted between 2012 and 2015 for banks. Whilst the scope of these visits is not explained in the reports published by the IOMFSA, the IOMFSA confirmed that the majority of banks were visited.

455. Whilst specific statistics in relation to AML/CFT visits are not available for earlier periods, the IOMFSA has explained that, taking account of risk: (i) banks are usually visited annually or every two years; (ii) fund and investment business licence holders are visited on a one to three year cycle; (iii) in a typical year, more than 40 on-site visits to TCSPs are conducted (with an average visit cycle of between 3 and 4 years); (iv) there are frequent visits to MVTS; and (v) a series of onsite inspection visits of life assurance companies has taken place since the last IMF inspection. All of these visits would have an element of AML/CFT compliance being assessed.

456. On-site visits conducted under the FSA 2008 and IA 2008 are not standardised. Instead, the scope of each review is set out in a bespoke visit planning memorandum and visits are designed to address key risks that have been identified. In some cases (investment business and services to collective investment schemes), the regulator now uses a "prompt sheet" (highlighting matters to be considered during an on-site visit), whilst still making it clear that judgment should be applied to focus on issues regarded as being material. In contrast, visits conducted under the DBRO Act follow a visit procedure. Inter alia, this sets out what should be tested on-site and factors that must be considered when testing client files.

457. Whilst the absence of specific statistics on AML/CFT visits (number and results) for earlier years has an impact on assessment of effectiveness in this area, results of themed visit programmes (banking and life assurance) and inspections of TCSPs for 2013 to 2015 point to an active supervisory approach, and confirm that compliance with a broad range of areas is tested on-site (from business risk assessments through to reporting of suspicion) based on sample files reviews.

GSC

458. The GSC's risk-based supervision of the gambling sector is recent (one week before the on-site visit), so the effectiveness of this mechanism cannot be assessed properly. The system also, as in the IOMFSA's case, takes into account various factors, including the outcomes of on-site visits, and data gathered from desk-based reviews. Under the previous system, the frequency and scope of on-site visits did not take ML/TF risk into account; instead visits were conducted as part of a rolling programme and the supervisory regime rarely penetrated cultural aspects of operators' systems. The figures below are for 2015, the first year since 2010 that specific AML/CFT on-site visits have been conducted.

459. The GSC uses detailed templates for on-site visits and desk-based reviews.

Table 13

Sector	Registered	Total number of on-site visits	Number of AML/CFT specific on-site visits	Number of combined on-site visits (AML/CFT and general)
Casino	1	9	0	5
Online gambling operators	39	72	48	22

460. The following table shows the number of "combined" visits (where AML/CFT compliance has been considered along with other matters).

Table 14

Sector	2014	2013	2012	2011
Casino	4	7	5	4
Online gambling operators	27	28	26	8

Lawyers and accountants

461. Under memoranda of understanding with the DHA, the Law Society and five UK accountancy bodies with members in the IoM, including the ICAEW and ACCA, oversaw compliance by their

members with the AML/CFT Code between 2010 and 2015. Under these memoranda, bodies undertook to monitor their members on the basis of "cyclical and risk-based visit selection". Given the relatively recent introduction of these arrangements, every practice was visited by the Law Society in three of the last four years, with a risk-based approach adopted only in the on-site visit programme for 2013 to 2014. The ICAEW is understood to have applied the same risk-based approach that is applied to its members in the UK. As noted elsewhere, supervision of both professions is now the responsibility of the IOMFSA under the DBRO Act.

462. The Law Society conducted 33 on-site AML/CFT visits in 2012, 35 in 2013, 24 in 2014, 30 in 2015 and 1 (so far) in 2016. Information is not available for accountants, except for 2012 when 5 combined visits were undertaken by the ACCA and 20 by the ICAEW.

Remedial actions and effective, proportionate, and dissuasive sanctions

IOMFSA

463. The range of sanctions available to the authorities is broad enough to deal with the types of FIs and DNFBPs found in the IoM. Sanctions range from written warnings followed by a remediation process (after an on-site visit) to withdrawal of a licence, and include fining powers. The main supervisory action used is a written warning followed by a remediation process. Action may also be taken against natural persons.

464. The following table provides information on the number of AML/CFT sanctions or other measures imposed by the IOMFSA in the period from 1 March 2014 to 28 February 2015, the first full year that information of this type was collected.

Table 15

Sector	Number of on-site visits covering AML#CFT	Number of visits identifying infringements	Written warnings	Directions and conditions
Banks	12	2	1	0
Funds and investment services	38	4	4	0
Life assurance (calendar year)	13	10	2	0
MSBs and exchange offices	3	2	2	1
Trust and company services providers	53	25	25	1

465. Prior to 2014, the IOMFSA has explained that extensive use was also made of written warnings (i.e. corrective action that is identified in a visit report) and very few cases were taken to the stage of enforcement (though, in a severe case, in 2011 there was a referral to the AGC). Given some of the more recent findings of the on-site visit process, evaluators consider this to be surprising. However, formalisation and re-focussing of the mandate of the IOMFSA's remediation panel (which decides what type of supervisory action is needed) in March 2014 should help now to ensure that the most appropriate cases are referred for enforcement action. Sanctions applied in 2015 by the remediation panel include action taken against two individuals who have been prevented from performing functions in relation to regulated activity subject to appeal and a third who has been given a written warning notice that there are grounds to believe that activities or circumstances are prejudicial to the IOMFSA's assessment of that individual's fitness and propriety.

466. Supervisory discretion is one of the pillars of creating a properly functioning supervisory regime and professional relationship between the supervisor and supervised institutions and the supervisor will take into account a number of factors when considering to use the ultimate sanction available to it – revocation of a licence. Use of such a power (or threat that it may be used) is recognised as one of the elements of supervision that creates a "culture of compliance" in the financial sector. The same is true also for the use of civil penalties, the legal basis for which was introduced under the FSA 2008 on 1 August 2015. The IOMFSA has explained that removal of a

licence can carry a risk of significant collateral damage to innocent customers and so prefers to appoint receivers, or managers, or to change senior management in order to protect customers and allow AML/CFT breaches to be thoroughly investigated and remedied. There are examples of this happening in practice in the IoM (though not always for AML/CFT reasons).

467. The maximum penalty that may be applied to entities registered under the DBRO Act (including lawyers and accountants) is GBP 1 000. Such a level of fine is not effective at ensuring future compliance by sanctioned entities or dissuasive of non-compliance by others. However, the IOMFSA has explained that other complementary sanctions may also be applied by the IOMFSA.

468. At the time of the on-site visit, there was a significant case-load in the enforcement section of the IOMFSA which consists of 4 full time members of staff. 30 cases were under on-going consideration and a further 6 dropped due to case priority and lack of resources. Significantly enough, over 60 individuals were subject to enforcement actions, out of which 47 were associated with the TCSP sector (the majority in relation to one case). Nevertheless, the evaluation team acknowledges actions taken by the IOMFSA enforcement division, and perceives them as prompt in cases where there was such a need.

469. More effective use of the IOMFSA's remediation panel and a better and more transparent decision-making process has increased the case referral rate to enforcement and this has created a problem of understaffing in this part of the IOMFSA.

470. Little has been seen in terms of enforcement against lawyers. Three matters have been referred by supervisors to the Council of the Law Society (one of which did not relate to AML/CFT) and just one matter considered by the Advocates Disciplinary Tribunal (independent of the Law Society) which was reluctant to take action. Under the DBRO Act, enforcement action will be taken in future by the IOMFSA.

471. No information has been presented to evaluators regarding any action taken in respect of accountants.

GSC

472. The GSC is unable to apply effective, proportionate and dissuasive sanctions. It is able only to revoke a licence of an online gambling operator or to direct that a director or other person exercising managerial functions be removed from their position or deprived of their function. The threat of use of these sanctions is used effectively by the supervisor (though it has not used these sanctions in practice); however, it should have the supervisory discretion to use other, less burdensome, sanctions. Unlike the IOMFSA, the GSC has not issued any written warnings (informal sanctions) during the period under review.

Impact of supervisory actions on compliance

IOMFSA

473. The IOMFSA appears to be well respected, and entities spoken to welcome the interaction they have with them. The IOMFSA has published a "supervisory approach" for all financial sectors, except for the insurance sector, to assist licence-holders' understanding of its work. The IOMFSA is also developing similar guidance for FIs and DNFBPs that are supervised under the DBRO Act.

474. The IOMFSA has explained that, where findings for a particular on-site visit are relevant also to other FIs, they are brought to the attention of those other institutions. The IOMFSA also publishes the results of its thematic reviews (banking and life assurance sectors). Both measures will have a positive impact on compliance. However, the IOMFSA does not consider trends in other on-site findings, e.g. over recent years. Accordingly it is not clear how it can measure whether its actions have led to improvements in overall compliance with the AML/CFT Code.

GSC

475. The GSC also appears to be well respected, and entities spoken to welcome the interaction they have with them.

476. Given the very recent introduction of a risk-based approach to supervision, it has not been possible to assess the additional impact of the GSC's supervisory model on compliance. The impact of supervisory actions would have been significantly more prominent had the GSC had a full range of sanctions at its disposal.

Lawyers

477. The Law Society has circulated a document each year to members setting out its supervisory approach for the forthcoming year. The approach has been approved by the Council of the Law Society and includes completion of an annual compliance return.

478. It has also produced an annual summary of findings from its on-site visit programme which considers areas where compliance has improved. The primary purpose of this summary is to highlight findings and themes which inform its oversight programme in the forthcoming year, and to provide support and guidance to members.

Promoting a clear understanding of AML/CTF obligations and ML/TF risks

IOMFSA

479. A primary forum for engagement with industry is through the Industry Advisory Group (formerly referred to as JAMLAG). The IOMFSA is a member of this Group and participates in all meetings (previously as the chair).

480. The main body of the AML/CFT Handbook was substantially redrafted in April 2015. Additional guidance on application of the AML/CFT Code by institutions in specific sectors was also published at this time. Publication of this sectorial guidance is to be commended. In particular, funds guidance explains the CDD measures that must be applied: (i) by the fund itself; and (ii) by fund service providers to the fund. At the time of the on-site visit, the IOMFSA was also well advanced in developing guidance for virtual currency operators. It is noted that the AML/CFT Handbook has not yet been updated to reflect findings in the NRA.

481. Given the use of complex ownership structures, it is explained under IO 3 that guidance is provided by the IOMFSA on: (i) information that could be obtained to understand the ownership and control structure of a customer; and (ii) who is to be considered the beneficial owner of a trust, covering matters such as "dummy settlors". This useful guidance could be clarified in some areas and perhaps consolidated.

482. Engagement also takes place through the IOMFSA's annual AML/CFT Conference and through outreach sessions to specific industry sectors. Relevant AML/CFT matters are also discussed in regular supervisory meetings held with industry bodies, e.g. the Isle of Man Bankers Association, Isle of Man Fund Managers Association, Financial Planners and Investment Brokers Association and the Association of Corporate and Trust Service Providers.

483. The IOMFSA uses outreach programmes to market participants, and is actively engaged with the industry. The IOMFSA has provided face-to-face training sessions to the DNFBP sector detailing the registration and oversight process to be followed as well as requirements under the applicable legislation.

484. The IOMFSA publishes the result of its thematic reviews (banking and life assurance sectors), the most recent of which was published in April 2016.

485. Overall, the evaluation team believes that the IOMFSA is taking action to promote a clear understanding of the AML/CFT obligations through the sectors. However, as noted under IO 4, the

extent to which FIs and DNFBPs (particularly banks) may be failing to meet the requirements in the AML/CFT Code to verify identity is not clear, given the differing evidence presented to the evaluators.

486. Interviews with the private sector did not always highlight a good understanding of ML/FT risk faced by particular businesses. This point is considered further under IO4.

GSC

487. The GSC published revised AML/CFT guidance for online gambling operators in December 2015 with case studies and examples.

488. The evaluation team understood from interviews with market participants that the supervisory outreach by the GSC is deemed useful. The relation with the supervisor was generally described by market participants as good, and mutual.

Lawyers

489. The Law Society has provided on-line training modules for use by advocates and non-legal staff since 2013 and is able to monitor usage by members. The Society also provides its members with free access to an external data source that can be used to conduct sanctions and PEP checks and to highlight negative media on potential and current clients.

Conclusion

490. **The IoM has achieved a moderate level of effectiveness for IO.3.**

CHAPTER 7. LEGAL PERSONS AND ARRANGEMENTS

Key Findings and Recommended Actions

Key Findings

• The extent to which legal persons and legal arrangements can generally be misused for ML/TF purposes is well understood. However, no exercise has been conducted 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.

• Whilst basic information is available online, the Central Registry does not collect all the basic information listed under c.24.3 (for foundations and partnerships) or collect it on a timely basis (for 2006 companies). The Registrar does not ensure that: (i) basic information provided to the Registry; and (ii) information recorded by legal persons on categories of shares, is accurate.

• Relevant authorities rely on: (i) TCSPs; (ii) nominated officers for 1931 companies; and (iii) companies themselves (in the case of 2006 companies) to hold all the necessary CDD information and evidence for companies. Beneficial ownership information for approximately 9,000 1931 companies that are not administered by a TCSP may not be adequate, accurate or current due to deficiencies in the framework in place.

• The authorities have not taken any specific measures to prevent the misuse of an unknown number of legal arrangements that are established under Manx law but which are only administered by foreign trustees or non-professional trustees in the IoM.

• Non-face to face business is common and many TCSPs take on business from professional intermediaries, e.g. law firms, without meeting their customer(s) (or beneficial owner(s)). Accordingly, where CDD information is provided by such intermediaries, there is an increased risk

that a TCSP may be provided with incomplete or false information and so not able to understand the nature of a customer's business and its ownership or control structure. This risk is greater still where there are information chains (see IO 4). This has an impact on the effectiveness of measures to prevent misuse.

• Some gaps in legislation have been identified in the TC annex, and addressing them will strengthen measures to prevent the misuse of legal persons and legal arrangements for ML/TF purposes. In particular, there are significant gaps in disclosure requirements for nominee shareholders and trustees.

• The Central Registry uses broad and effective sanctions against registered companies.

Recommended Actions

• In line with risks identified in the NRA, the authorities should take additional measures to address risks presented where TCSPs use CDD information provided by professional intermediaries.

• Authorities should also take measures to satisfy themselves that companies, shareholders and nominated officers comply with requirements set in the CBO Act 2012 in order to ensure that accurate and current beneficial ownership information is available to the authorities.

• Authorities should require trustees of express trusts governed under IoM legislation to obtain and hold information in line with c.25.1 and disclose their status to FIs and DNFBPs.

• Based on actual cases in the Isle of Man, threats presented by the use of legal persons and legal arrangements established under Manx legislation should be identified in order to strengthen the risk mitigating framework.

• 2006 companies, foundations and partnerships should be required to file all basic information (in line with c.24.3) on a timely basis with the Central Registry. More generally, basic information, along with information on categories of shares (including nature of associated voting rights) (held in line with c.24.4), should be checked for accuracy.

• Technical deficiencies identified in the TC annex should be addressed.

The relevant Immediate Outcome considered and assessed in this chapter is IO5. The recommendations relevant for the assessment of effectiveness under this section are R24 & 25.

Immediate Outcome 5 (Legal Persons and Arrangements)

491. As indicated in the TC annex, the process for the creation of legal persons and for obtaining and recording basic information is set out in the Companies Act 1931 to 2004, Companies Act 2006, Limited Liability Companies Act 1996, Foundations Act 2011 and Partnership Act 1909.

492. The Companies Act 2006, Limited Liability Companies Act 1996 and Foundations Act 2011 all mandate the appointment of a registered agent – a TCSP that is regulated and supervised by the IOMFSA - which is required to apply CDD measures to its customer(s)(and beneficial owner(s)) in accordance with the AML/CFT Code. CSPs have been regulated and supervised in the IoM since 17 October 2000 and TSPs since 13 July 2005. Unlike in many other jurisdictions, regulation is not limited to compliance only with AML/CFT legislation, and extends to prudential matters and conduct of business. The IOMFSA (and its predecessor) also proactively supervises the sector for AML/CFT compliance.

493. The Companies (Beneficial Ownership) Act 2012 establishes a requirement for companies incorporated under the Companies Act 1931 to 2004 (1931 companies) to disclose information on the beneficial ownership of such a company to a person nominated by the company (a "nominated person").

494. In order to enhance the transparency of legal persons and legal arrangements, the IoM has recently committed to holding adequate, accurate and current beneficial ownership for corporate

and legal entities. This information will be held in a secure electronic database (or similar). The Government has also given a commitment to embrace the G5 initiative on automatic exchange of beneficial ownership information[61].

Public availability of information on the creation and types of legal persons and arrangements

495. Information on the various types, forms and basic features of IoM legal persons is found in relevant laws, which are publicly available via the IoM Government Online Legislation website provided through the AGC and through the Central Registry. These laws are supported by a number of useful guides and practice notes which provide information on the creation and types of persons and arrangements found in the IoM. These guides and practice notes do not explain the process to be followed for obtaining and recording beneficial ownership information for all legal persons.

Identification, assessment and understanding of ML/TF risks and vulnerabilities of legal entities

496. The authorities understand the risk that legal persons and legal arrangements can be misused for ML/TF purposes. They have provided evaluators with a case study on evasion of value-added tax that included an IoM company, referred to the extensive use of IoM companies to hold real estate in London, and highlighted the use of Manx corporate structures in investigations started after the Arab Spring. Following publication of the Panama Papers, the IOMFSA wrote to all regulated entities (including TCSPs) requesting information on any relationships between such entities and the Panamanian law firm involved. In recognition of risks presented, the CED has also raised awareness and provided information on the use of corporate vehicles in trade-based money laundering. Moreover the IOMFSA has published detailed guidance for TCSPs (a section in the AML/CFT Handbook) which lists some higher risk features of corporate structures to be taken into account, and which provides examples of where overseas companies and trusts have been used to conceal beneficial ownership and to facilitate money laundering. The NRA also concludes that the form of legal person or legal arrangement that is selected is not considered to be a major component of AML/CFT risk (i.e. all legal persons and legal arrangements have features that present vulnerabilities).

497. However, the authorities have not systematically analysed cases where Manx legal persons and legal arrangements have been used to launder the proceeds of crime, notwithstanding the use by non-residents of IoM companies, nor risk presented by their use separately considered in the NRA (or comprehensively elsewhere), though there is an assessment of risks of vehicles to be found under the assessment of the TCSP sector (which administers many of the legal persons and legal arrangements that can be formed under Manx legislation).

498. It is said in the NRA that the closure of legal tax avoidance and planning opportunities for middle earners has led TCSPs to focus on wealthy clients and a more international client base, which is more likely to be politically exposed and to increase risks of receiving the proceeds of foreign corruption or organised crime. There is reference also to the misuse of vehicles to evade tax featuring highly in international experience of TCSP risk. The "availability of non-face to face transactions" – cases where a TCSP does not meet its customer – is also said to increase vulnerability.

499. Whereas the NRA assesses the risk of the TCSP sector as "medium high", TCSPs met on site downplayed the risk, and considered their products and services to present a low or standard risk.

[61] The IoM Treasury has published a consultation paper on the Beneficial Ownership Bill 2017. The authorities have explained that this Bill will address the technical deficiencies identified in the TC Annex.

Mitigating measures to prevent the misuse of legal persons and arrangements

500. There are two key elements to measures to prevent the misuse of legal persons in the IoM.

501. The first measure is a requirement that all companies (except 1931 companies) and foundations must have a registered agent - which must be a TCSP that is regulated and supervised by the IOMFSA[62]. Accordingly, that TCSP will be required to apply CDD measures to its customer(s) (and beneficial owner(s)) in line with the AML/CFT Code. This extends to the natural person behind any legal person.

502. The second measure is that, except where an exemption applies, 1931 companies (many of which are locally owned and managed trading companies with a substantial "footprint" in the IoM) must appoint a nominated officer – a person resident in the IoM – to hold information on beneficial ownership, in any case where the registered holder of shares is not also their beneficial owner. Accordingly, beneficial owner information for Manx companies will be held by TCSPs or nominated officers.

503. According to the NRA, non-face to face business is common and many TCSPs take on business from professional intermediaries, e.g. law firms without meeting their customer(s) (or beneficial owner(s)). Accordingly, where CDD information is provided by such intermediaries, there is an increased risk that a TCSP may have incomplete or false information and so not able to understand the nature of the customer's business and its ownership or control structure. This risk is greater still where there are information chains (see IO 4). This is an important point since the vast majority of information collected on beneficial ownership of legal persons and legal arrangements is held by TCSPs.

504. In the case of 1931 companies, whilst the concept of appointing a nominated officer is sound, a number of important deficiencies have been identified under c.24.6. In particular, it appears that a legal person may be the beneficial owner of a 1931 company. The mechanism is also reliant upon disclosure of information by the registered shareholder who in some cases may be: (i) resident overseas (and so requirements may not be enforceable); and/or (ii) unable to find out who is the beneficial owner (perhaps because there is a complex ownership structure and, unlike a TCSP, the registered shareholder does not have the skills to penetrate ownership of such a structure). Also, the regime does not apply to all 1931 companies, e.g. public companies that are permitted (by their articles) to invite the public to subscribe for shares or debentures therein. The authorities have explained how companies (but not also registered shareholders) are made aware of their statutory responsibilities and the Registrar has confirmed that he does not oversee compliance by shareholders with this disclosure requirement (which would in any case be extremely difficult). For example, a registered shareholder that is acting in a nominee capacity may not identify the actual nominator, or may identity a person who is not the beneficial owner (e.g. another nominee).

505. These deficiencies may be mitigated where: (i) a TCSP is involved in the administration of a 1931 company (which is the case for over half of 1931 companies); and/or (ii) where a 1931 company is owned and operated by IoM (rather than overseas) residents.

506. There is no register or record of general partnerships in the IoM. Limited partnerships are not required to have a registered agent (a TCSP that is regulated and supervised by the IOMFSA). They are, however, required to have a place of business in the IoM and to appoint an IoM resident who is authorised to accept service of documents and anyone providing a place of business by way of business has to be regulated and supervised by the IOMFSA. However when a limited partnership is formed by a non-resident without any TCSP connection, beneficial ownership may not be readily

[62] In the case of a LLC, the Limited Liability Companies (Registered Agents' Qualification) Regulations 2003 do not include such a requirement, though the effect of the RAO 2011 will be to require such an agent to hold a class 4(5) licence where the agent is acting by way of business. In practice, it is expected that most agents will be acting by way of business.

available in the IoM (though it may be accessed through a person who must be resident in the IoM to accept service of documents). In practice, it is thought that most limited partnerships will have a TCSP connection, though statistics have not been presented to support this. Given the limited use of partnerships (including partnerships), evaluators do not consider these deficiencies to be significant.

507. Like many other jurisdictions that recognise trusts, the authorities have not taken any measures to prevent the misuse of legal arrangements that are established under Manx law but which otherwise have no nexus with the IoM. The IoM does not require trustees of express trusts governed under the Trustee Act 2001 (including Unit Trusts that are exempt scheme) to obtain and hold information on the identity of the settlor, trustee, protector and beneficiaries where the trustee: (i) is not resident in the IoM; (ii) is resident in the IoM but is not a professional trustee; or (iii) in the case of an exempt scheme, does not have a resident manager.

508. Bearer shares are not an issue in the IoM and are prohibited under the Companies Acts 1931 to 2004 and Companies Act 2006. Currently only one company with bearer shares is registered, and this is because it was reinstated to the register at the request of the IOMFSA (for the purpose of court action) and is under their scrutiny. As such it presents no risk.

509. All persons acting as nominee by way of business in the IoM must be licensed as TCSPs under the FSA 2008 to carry on business[63] there and are subject to the AML/CFT Act (which requires them to maintain information identifying their "nominator"). However, they are not required to disclose to the Central Registry the capacity in which they hold shares or other interests in a legal person established in the IoM. As described above, measures are in place to require registered shareholders of 1931 companies to disclose their nominator to a nominated officer, but this information is not also recorded at the Central Registry.

Timely access to adequate, accurate and current basic and beneficial ownership information on legal persons

510. Legal persons are required to notify the Central Registry about any prescribed changes to information, generally within one month of the change occurring. Not all legal persons are required to provide all basic information to the Registrar. Notwithstanding this, competent authorities can obtain any information that is not held on the public register through statutory powers.

511. The Central Registry does not have responsibility for checking the accuracy of basic information provided to it, though its publication will allow the public to identify circumstances where there are errors. However, it does conduct checks on documents filed by companies, in order to enforce compliance with filing requirements, including timely delivery of documents, and applies pecuniary sanctions (late filing fees) and strikes-off companies from the register (the latter as part of the annual return process). In particular, the Registrar will reject an annual return when basic information has not been updated by a company during the year.

512. As noted above, the authorities rely on TCSPs that are regulated and supervised by the IOMFSA or nominated officers to hold adequate, accurate and current information on the beneficial owners of companies.

513. The effect of requirements placed on TCSPs should be to ensure that adequate, accurate and current beneficial ownership information is available on a timely basis. However, the non-face-to-face nature of many relationships, use made of professional intermediaries, and tendency of TCSPs interviewed to downplay risk (with consequent effect on application of commensurate CDD measures) will have an impact on the effectiveness of such requirements. A particular case identified by a supervisory examination conducted by the IOMFSA also highlights a number of examples of

[63] CSPs have been regulated and supervised in the IoM since 17 October 2000.

where such data was not collected[64]. The IOMFSA's supervision of TCSPs has also identified some instances where CDD requirements have not been properly applied – see IO 4.

514. Deficiencies in measures in place to address risks for 1931 companies are described above (followed by some factors that may mitigate those deficiencies). In addition, the nominated officer is not required to hold on to information provided by registered shareholders for any period of time (no retention period) and changes in beneficial ownership data may be disclosed to the nominated officer up to 3 months after the change, which impacts the effectiveness of the regime.

515. Other than for limited partnerships, beneficial ownership information will be requested from the registered agent (whose details are publicly available at the Central Registry) or the nominated officer (whose address is publicly available at the Central Registry). Every limited partnership is required to maintain a place of business in the IoM and to appoint one or more persons resident in the IoM to accept service. If beneficial ownership information is required, a production order can be served on the person appointed to accept service or to the general partner at the place of business. However, as noted above information may not be held in the IoM and may not be adequate, accurate or current. Basic information will be accessed through the Central Registry or legal person itself.

516. All basic and beneficial ownership data held is available to the authorities (using statutory powers), and they have used their powers on many occasions to request such information, e.g. in response to requests from overseas tax authorities. The vast majority of requests for beneficial ownership information have been sent to banks and TCSPs. Responses have been provided to all requests since 2008 for supervisory assistance in respect of beneficial ownership information and, since 2010, there have been only three occasions (all requests – including beneficial ownership) where it has not been possible to execute a LOR for domestic reasons. Where this information is requested under MLA, witnesses are summonsed to court to give evidence, answer questions and produce documentation in relation to beneficial ownership. The FIU and FCU cannot recall any cases where they were unable to obtain beneficial ownership information for intelligence gathering or investigation purposes.

Timely access to adequate, accurate and current basic and beneficial ownership information on legal arrangements

517. With respect to legal arrangements, information on the beneficial ownership of a trust established under Manx law will be held in the IoM where the trust is administered by a TCSP (as for legal persons). Where a trustee is resident in the IoM but: (i) does not carry on that activity by way of business; or (ii) acts in relation to a small domestic trust (the gross assets of which do not exceed £5,000), there is no requirement to hold information in the IoM.

518. No general obligation is placed on trustees of IoM trusts to collect beneficial ownership information and so authorities in the IoM and elsewhere may not be able to secure adequate, accurate and current information where the trustee is not subject to the AML/CFT Code, e.g. the trustee is resident outside the IoM.

519. In order to find out which TCSP holds information on trusts administered in the IoM, the IOMFSA would send a mail-merge message to all TCSPs requesting them to identify themselves. Sanctions would apply to any TCSP who failed to comply. However, most enquiries regarding trusts come with a known address for the service of mail, which is usually the address of a TCSP and so will be known to the IOMFSA. It is rarely a problem identifying who administers a trust. Often the name of a trustee will also identify to the IOMFSA which TCSP is involved if they provide that trustee.

[64] The authorities have said that this case is not typical of the sector as a whole.

Effectiveness, proportionality and dissuasiveness of sanctions

520. If a notification is delivered to the Central Registry outside the prescribed filing period, a late filing fee is charged depending on how late the notification is delivered. The application of such filing fees is considered by the Registrar to be dissuasive. If an annual return is not delivered for a company, the Central Registry will also take action to remove the company from the register. The threat of striking off a company is taken seriously as the cost of restoring it is significant and can deprive members of enjoyment of assets.

521. The Registrar has applied pecuniary fines in practice (over GBP 1 million has been collected in late filings fees since January 2014) and has removed over 2,000 companies from the register for not filing an annual return within six months of the filing date between 2011 and 2013[65].

	Action commenced	Number struck off Register
1931 Companies		
2011	1463	657
2012	1450	701
2013	965	409
2006 Companies		
2012	257	137
Jan 2013	218	93
Dec 2013	253	99

522. No sanctions have been applied to registered shareholders of 1931 companies for failing to disclose information to the nominated officer because no instances of non-compliance have been identified. However, as described above, the Registrar has confirmed that he does not oversee compliance by shareholders with this disclosure requirement.

523. As set out under IO 3, the IOMFSA has explained that extensive use has been made of written warnings (i.e. corrective action that is identified in a visit report) in earlier periods. Given some of the more recent findings of the on-site visit process, it is considered that there has been over-reliance in the past on the use of remediation plans to address AML/CFT deficiencies. Accordingly, sanctions applied to enforce compliance by TCSPs have not been proportionate and dissuasive.

Conclusion

524. **The IoM has achieved a moderate level of effectiveness for IO.5.**

CHAPTER 8. INTERNATIONAL COOPERATION

Key Findings and Recommended Actions

Key Findings

• The IoM provides constructive and, in most cases, timely MLA across a range of international co-operation requests.

• There are no formal guidelines setting out the criteria to prioritise requests to ensure both more effective investigation and prosecution of ML/FT and, in particular, restraint and confiscation of criminal proceeds especially, in the early stages of a criminal investigation. Due to the relatively small number of requests handled by the international cooperation team, prioritisation is done on a case-by-case basis.

• Excellent cooperation exists between the IoM and the UK, especially with regard to tax and customs matters. The UK regularly disseminates SARs reported in the UK to the IoM, which are then

[65] On 25 April 2016, strike off action was commenced against a further 1,770 1931 companies.

examined by competent authorities. Examples of effective cooperation have been presented to the evaluators both with regard to on-going criminal investigations, and enforcement of targeted financial sanctions.

• The IoM proactively seeks legal assistance and other forms of international co-operation from the UK. Nevertheless, it has not done so systematically with other jurisdictions to pursue domestic ML, associated predicate offences and TF cases which have transnational elements, or for the detection of potential funds or assets which are owned or controlled, directly or indirectly, by sanctioned persons or entities. This is considered to be a significant weakness in the system, since it is one of the few avenues available to the authorities, which could assist them in initiating domestic ML related to foreign predicate offending. Mechanisms and procedures are not yet in place for enabling and ensuring the effective harvesting and use of information included in incoming MLA requests.

• Generally, foreign FIU counterparts have provided positive feedback on the FIU`s ability to provide requested information, including information on beneficial ownership. However, some counterparts referred to cases where the FIU urged the requesting FIU to collect the requested information through the application of MLA since the FIU, during much of the period under review, did not have the power to compel the production of information by reporting entities where such information was not already contained within its database. It is understood that in many cases the FIU has sought to find pragmatic solutions to circumvent the limited powers to request additional information from reporting entities in the absence of a SAR.

• Overall, in the context of an international financial centre, the low number of outgoing requests does not seem commensurate with the IoM risk profile and level of intelligence generated domestically and confirms the lack of a proactive approach.

Recommended Actions

• The authorities should develop both a strategy and written policies to ensure systematic proactive seeking of foreign assistance (including elements of assets seizure and restraint) in all available channels upon suspicion of ML/TF or violation of targeted financial sanctions.

• The authorities should review the MLA framework. Formal prioritisation criteria should be established, Additional resources should be allocated to the international cooperation unit once the number of proactive requests increases to ensure both effective investigation and prosecution of ML/FT and, in particular, restraint and confiscation of criminal proceeds especially in the early stages of a criminal investigation.

• A more sophisticated case management system should be appropriately developed to ensure the timely prioritisation of all MLA requests.

• The authorities should also use as a policy objective the existing powers to actively assist foreign jurisdictions in identification, repatriation, sharing or restitution of criminal proceeds and instrumentalities located in the IoM.

• The FIU should use the powers granted under the new FIU Law to effectively provide requested information, including information on beneficial ownership, in the pre-investigative stage prior to MLA.

• 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.

The relevant Immediate Outcome considered and assessed in this chapter is IO2. The recommendations relevant for the assessment of effectiveness under this section are R.36-40.

Immediate Outcome 2 (International Cooperation)

Providing constructive and timely MLA and extradition

a) Location and Extradition of Criminals

525. Although a small number of requests for assistance in locating individuals have been received since 2009, in each of those cases it transpired that the requests were made as a result of criminals giving a false address in their jurisdiction. In more complex cases, further enquiries would be carried out, and the tools available to the AGC in this regard include applications to court in respect of FIs, such as customer information orders (revealing whether an account is held in the IoM) and account monitoring orders (revealing any transactions made on the account), under POCA.

526. The IoM has not carried out any extraditions within the period under review. In fact, there has never been a formal extradition to or from the IoM, at least not within living memory.

527. However, rarely, the issue does come up. The current extradition regime in the IoM is suitable for its purpose, although the current development of a domestic Extradition Bill is an indication that the IoM would wish to have more control over the procedure of any such extradition, were it to occur in the future.

b) MLA

528. The AGC is the Central Authority in the IoM responsible for making and receiving MLA requests in respect of investigation and prosecution of crime, criminal asset tracing, restraint and confiscation, and civil recovery (non-conviction based confiscation). The Attorney General is assisted in dealing with incoming letters of request ("ILORs") by a full-time qualified lawyer within AGC with the title "Legal Officer, International Cooperation".

529. The AGC is assisted by the FIU, and in some cases, the FIU has dealt with preliminary enquiries from the requester, or has spontaneously provided intelligence which forms the basis of the request.

530. There are no formal rules directing the method by, or timeframes within which, MLA requests should be executed. Requests are dealt with as expeditiously as possible, taking into account AGC and court resources, and the time required by witnesses for preparation. At present, a turnaround time of no longer than four months is the aim, with urgent cases being prioritised within the AGC, and executed as soon as court and witness availability allows. This flexibility allows each request to be dealt with by the most efficient and appropriate method, with specific regard to its nature and circumstances. The majority of cases are executed within four months. The table below shows an average turnaround time of 70.6 working days over the past six years.

531. There are no binding policies or guidelines regarding grounds for refusal of assistance and very few instances in which assistance will not be granted. One of the most common reasons for an ILOR to remain unexecuted is that the information sought no longer exists or, more often, was never held in this jurisdiction.

*(working days to execution, notification that unable to assist or withdrawal)

Table 16							
	Total including supplementary requests	Executed in full	Unable to assist as no evidence held in IoM	Unable to assist due to domestic reason	Unable to assist / LOR withdrawn due to defect in LOR	Pending / On-going	*Turnaround time
2010	54	43	1	1	9	0	54.6
2011	80	65	6	0	9	0	67.6
2012	82	69	5	1	7	0	79.1
2013	84	61	12	1	9	1	70.6
2014	63	46	11	0	3	3	74.9
2015 to 18.11.15	50	25	3	0	6	16	76.8

Since 2010, it has not been possible to execute an ILOR for legal restrictions on only three occasions, due to objectives reasons.

532. As reported by the authorities the main reason for non-execution of ILORs is that they are, in their view, defective, or they are withdrawn, and this situation has arisen 43 times since 1 January 2010. It is not uncommon to receive no response to a request for further details (for example, confirmation that a criminal investigation or prosecution is underway, or more information in relation to the connection to the IoM). In addition, ILORs in relation to more minor offences (commonly credit card theft involving online gaming) may be withdrawn as the information can be provided swiftly on a police-to-police basis instead.

533. On 38 occasions during that period, it has not been possible to execute a request as no relevant information was held in the IoM. Often bank accounts believed to be held within the IoM are actually in the UK or Channel Islands.

534. Notwithstanding the fact that there are no clear guidelines as to the prioritisation in dealing with incoming requests, ILORs for restraint are given priority as a matter of course. This is evidenced by an average turnaround time for restraint of 18.8 working days, as opposed to the turnaround time of between 54.6 (2010) and 79.1 (2012) working days for all requests (see Table 16).

c) Identification of Assets and Provision of Information (Including Evidence and Information regarding Beneficial Ownership)

The majority of requests received are for information and/or evidence.

Table 17							
Nature of assistance requested	2010	2011	2012	2013	2014	2015*	Total (in 6 years)
Obtaining documentary evidence	49	74	75	77	56	44	375
Restraint	5	4	3	3	2	0	17
Confiscation	0	0	1	1	3	2	6
Service of process	0	1	0	3	2	0	6
Facilitate witness giving evidence in trial (by video link or attendance)	0	1	0	0	0	2	3
Permission to share documentary evidence with another jurisdiction for joint investigation	0	0	2	0	0	2	4
Total	54	80	82**	84	63	50	412

*to 18 November 2015

**including one request for taking of a DNA sample not shown in this table.

535. Methods can include production orders, customer information orders and account institutions. Most can be used to obtain fiduciary information and evidence, including that relating to beneficial ownership, from TCSPs. By far the most common method for executing such requests is under section 21 of the Criminal Justice Act 1991. Upon request, the Legal Officer International Cooperation produces a draft court summons which is referred to the witness so that any issues they may have with the request can be resolved.

536. To date (since 2009) there have been no instances of the Attorney General or the High Bailiff refusing to grant assistance to foreign requests.

537. The Legal Officer, International Cooperation also facilitates the provision of publicly available information and voluntary witness statements in response to ILORs and less formal requests from counterparts in other jurisdictions. As a matter of course, where an ILORs information from the Companies Registry, a link to the Companies Registry website, is provided in the letter of acknowledgement sent within three working days of receipt of the letter. Although the AGC's involvement in the taking of voluntary witness statements and conducting of voluntary interviews is limited, assistance is offered and given (in conjunction with the FIU) in relation to ascertaining witness availability, providing interview rooms and, if necessary, facilitating use of the video conferencing facilities at the IoM Courts of Justice.

538. ILORs are all sent to the International Cooperation Unit of the FIU, which can cross-reference the details with information in its database. Should further information be identified, the FIU would inform the Legal Officer, International Cooperation who would alert the requesting authority. as would the FIU to its foreign counterpart. The evaluation team, however, is of the view that the IoM, when requested to provide documentary evidence at the request of a foreign country should be more proactive in searching for additional assets that the foreign requesting country is unaware of, especially, if the requesting country might not have the knowledge to understand what to ask for when complex structures are involved.

539. The following table sets out the offences in relation to which ILORs have been received over the past six years:

Table 18						
	2010	2011	2012	2013	2014	2015*
Money Laundering ("ML")	5	9	5	7	8	3
ML + Corruption	8	5	2	4	2	2
ML + Fraud	0	8	13	15	14	6
ML + Drugs	4	9	5	1	0	0
ML + Tax Evasion	0	1	3	0	2	4
ML + Organised Crime	0	2	0	0	0	3
Terrorist Financing	0	1	0	0	0	
Corruption	5	4	6	4	3	5
Tax Evasion	6	8	4	8	5	4
Fraud	9	15	19	24	17	14
Drugs	0	0	8	4	1	2
Other	17	18	17	17	11	7
Total Requests	54	80	82	84	63	50

*to 18 November 2015

540. Where the LOR refers to more than one offence (other than in the case of ML with certain predicate offences which have been added as extra categories) the main or most serious offence has been noted here.

d) Freezing / Restraint of Assets

541. The authorities prioritise requests for restraint of criminal assets (or suspected criminal assets). As requests of this nature must include more detailed information than is required in a

request for information or evidence, if necessary, full guidance is provided to the requesting authority. Requests are acknowledged, and further information sought if necessary, as soon as possible upon receipt of the original letter.

542. Restraint orders are made by the Court of General Gaol Delivery (the higher criminal court) following an ex parte application made by the Legal Officer, International Cooperation heard by a Deemster. If granted (and there are no instances of refusal within the last six years, or indeed longer) the order is served upon the suspect / defendant, but no prior notice of the application or hearing is given.

543. Dual criminality is required, but the conduct underlying the offence, rather than the terms in which it is expressed in the legislation of the requesting country is considered when determining whether dual criminality exists.

Requests for External Restraint Orders to be registered in the IoM

Table 19			
	Jurisdiction	Offence	Turnaround Time (working days from receipt of LOR)
2015	1 Spain	Fraud	69
2014	1 USA	ML & Fraud	9
2013	1 Kyrgyz Republic	Corruption	23
	2 England and Wales	ML & Fraud	15
2012	1 England and Wales	Other (internet sales of prescription only drugs)	6
	2 Australia	Money Laundering	32
	3 US	Securities Fraud	22
2011	1 US	Securities Fraud	22
	2 England and Wales	Fraud	2
	3 England and Wales	ML & Drug Trafficking	4
	4 England and Wales	ML & Drug Trafficking	80
2010	1 England and Wales	Corruption	12
	2 England and Wales	ML & Drug Trafficking	48
	3 England and Wales	Customs and Excise Tax Offences	23
	4 England and Wales	Corruption	3
Average turnaround time - 18.8 working days from receipt of request			

544. Requests for restraint are often withdrawn following a request for the information needed in order to make an application to court. The authorities take the view that this is not a result of particularly onerous requirements in the IoM (which are in line with requirements in the UK), but rather an absence or lack of necessary information contained in a request such as, details of the person and authority in the requesting jurisdiction making the request, full details of the individual/individuals suspected of committing a criminal offence, etc.

545. In each case where the original letter of request does not contain sufficient information, the Legal Officer, International Cooperation will enter into correspondence or dialogue with the requester, to ensure that an application with good prospects of success is made wherever possible. Once a restraint order has been made, the matter is reviewed from time to time with updates requested from the requesting jurisdiction.

e) Confiscation and Civil Recovery (non-Conviction Based Confiscation)

546. As with requests for restraint, a more detailed letter of request is required for confiscation. Confiscation on behalf of another jurisdiction is given effect by registration of the foreign confiscation order, by a Deemster in the Court of General Gaol Delivery (the higher criminal court), as an external order under the Proceeds of Crime (External Requests and Orders) Order 2009.

547. Notice of the registration of the order is served upon the defendant (and other affected parties, such as those purporting to be joint owners and the FI holding the asset) and then a subsequent order is made for enforcement of the confiscation order. As in restraint applications, the application is made by the Legal Officer, International Cooperation acting as advocate for the requesting authority, on behalf of the Attorney General.

Requests to the AGC for External Confiscation Orders to be registered in the Isle of Man

	Jurisdiction	Offence	Isle of Man Asset(s)	Turnaround Time (working days from receipt of LOR)
2015	1 England and Wales	Corruption	Three bank accounts with a total balance of £50,676.27	20
NB. Non-conviction based confiscation requested	2 England and Wales	C&E Tax Offences	Funds (amount unknown) believed to be held in bank account in Isle of Man	211
2014	1 England and Wales	Fraud	30% of net equity in property in Isle of Man	N/A
	2 England and Wales	ML & Fraud	£56,490.69, representing the value of shares in a liquidated company	123
	3 England and Wales	Money Laundering	Land in UK owned by IoM company	N/A
2013	1 England and Wales	Fraud	£12,636.38 held in bank account in Isle of Man	178
2012	1 England and Wales	C&E Tax Offences	Bond Policy held in Isle of Man, confiscation to the value of £304,317.62	26
2011	0			
2010	0			
Average turnaround time: 111.6 working days from receipt of request				

548. A regime for non-conviction based confiscation, referred to as "civil recovery", is set out in the Proceeds of Crime Act 2008 and can be applied in cases of MLA requests by virtue of the Proceeds of Crime (External Requests and Orders) Order 2009. To date, only two such requests have been received. A request received from England and Wales in 2015 was withdrawn as the investigation in that jurisdiction was discontinued. An earlier request, contained in a letter dated 13 November 2009, was successfully executed in 2010 and is described in the case review below.

f) MLA conclusion

549. The IoM has generally provided constructive and timely MLA and, potentially, extradition across the range of international co-operation requests. Most countries which provided feedback on their experience regarding cooperation with the IoM commented positively on both the swift responses and their good quality.

550. An 18 days average for processing restraint requests and an average of 111 days for dealing with external confiscation orders appear to be a relatively efficient turnaround.

Seeking timely legal assistance to pursue domestic ML, associated predicate and TF cases with transnational elements

551. The authorities do not, on a regular and systematic basis, seek legal assistance for international co-operation (other than with the UK) in an appropriate and timely manner to pursue

domestic ML, associated predicate offences and FT cases which have transnational elements. During discussions with the authorities, the evaluators have come across several examples where such enquiries have not been made.

552. Outgoing letters of request ("OLORs") for MLA are drafted by the Legal Officer, International Cooperation in accordance with instructions received from and investigating officer or Prosecutor. Once approved and signed by the Attorney General they are sent directly to the central authority of the requested jurisdiction.

553. The International Cooperation Unit of the FIU is staffed by two officers. They undertake a wide range of assistance to other LEA's outside of the IoM including assisting the Attorney General with ILOR.s

554. Analysis of the table below summarizing OLORs substantiates the evaluators' conclusion as to the lack of pro-activeness by the authorities. There were 7 outgoing requests (regarding only 3 cases) in 2015 and none in 2014, 2012 and 2011.

OLORs 2010 – 2015 (to 18 November 2015)

Table 20		
	Requested Jurisdiction	Offence(s) in IoM
2015	1 British Virgin Islands	Theft, false accounting, forgery and conspiracy to obstruct justice
	2 Bahamas	As above
	3 Cyprus	As above
	4 Scotland	As above
	5 England and Wales,	Fraudulent evasion of VAT
	6 England and Wales,	As above
	7 England and Wales,	Grievous bodily harm
2014		
2013	1 Germany	Causing death by careless driving
	2 Bahamas	Theft, false accounting and forgery
2012		
2011		
2010	1 England and Wales, 04.02.10*	Theft, false accounting and money laundering
	2 England and Wales, 08.02.10	Fraudulent evasion of VAT and money laundering
	3 England and Wales, 16.11.10	As above (supplementary request)

* all relate to the same long-running theft investigation involving a corporate service provider from which client funds were stolen.

The international cooperation within the MLA framework is predominantly tied to the UK with no evidence of efforts made to seek MLA engagement with jurisdictions which have been the subject of suspicions activity reporting (e.g. UAE - 34 STRs/0 MLA; Hong-Kong - 26 STRs/0 MLA; Italy – 23 STRs/1 MLA; Nigeria 21 STRs/0 MLA).

555. This lack of pro-activeness has in the eyes of the evaluators a strong negative effect on effectively combating potential and existing suspicion of complex ML on the IoM. Most of both the ML suspicions and cases discussed with the local authorities involve structures created on the IoM with several international elements such as foreign UBO, transaction with foreign FI and additional foreign corporations which are part of the IoM structure. Refraining from proactively and systematically seeking information from all these foreign jurisdictions hampers the ability of successful detection investigation and prosecution of ML.

Seeking other forms of international cooperation for AML/CTF purposes

GSC

556. Memoranda of Understanding ("MOUs") are in place between the GSC and 6 other gambling regulators to control requests for information for both personal and generic information. Additional MOUs are in place between the GSC and certain other sporting and sports integrity agencies in respect of generic information related to match fixing and sports integrity issues[66].

557. The GSC does not keep statistics on the numbers of information requests sent and received within the context of international cooperation. The authorities, however, indicated that the volumes of requests made and received are low and are easily managed by one staff member, the Director of Licensing and Compliance. The GSC is predominantly a requested rather than a requesting authority.

IOMFSA

558. The IOMFSA does not need to have a co-operation agreement in place in order to seek and provide assistance. Nevertheless, the IOMFSA has entered into many co-operation arrangements. The IOMFSA is a full signatory to the IOSCO Multilateral Memorandum of Understanding ('IOSCO MMOU') under which it co-operates and exchanges information for the purposes of regulatory enforcement of securities matters. As well as detailing the type of co-operation required by signatories, the IOSCO MMOU ensures that no domestic laws or regulations can prevent securities regulators from sharing information with their counterparts in other jurisdictions.

559. The IoM is one of 54 signatories (at the time of writing) to the IAIS MMOU which is a global framework for cooperation and information exchange between insurance supervisors. The IOMFSA has entered into 27 Co-operation Agreements under the EU's Alternative Investment Fund Managers Directive. In addition, the IOMFSA has over 30 regulatory and supervisory MOUs. The Annual Report of the former FSC for the year ended 31 March 2015 recorded that over the period of the report, the FSC sent 130 letters to other supervisors for regulatory purposes, and received 83. The IOMFSA is a member of and participates in a number of supervisory colleges in respect of groups of which IoM insurers are members and liaises with supervisors in the IoM and elsewhere about matters of common interest including systemic risk, group-wide solvency, exposure to ML/FT risks and group crisis management plans. The IOMFSA is also a member of a UK based regulatory and law enforcement forum which meets every 6 weeks to discuss emerging fraud and criminal trends and to consider how best to deal with them.

FIU

560. The FIU has been a member of the Egmont Group (since 2001) and exchanges information regularly with foreign counterparts. Since 2013 the IoM has received 185 requests from Egmont and sent 18. During the on-site visit, the assessment team was advised that most communications dealt with UK related cases and therefore the UK-FIU (NCA) is viewed as the main partner in exchanging financial intelligence internationally. Looking at the numbers dating back to 2009 the FIU, on average, seeks financial information around seventy (70) times per year which is a significantly smaller figure compared to the approximately two hundred (200) requests it receives per year. Most cases where the FIU takes a pro-active approach deal with the UK.

FCU

561. The FCU cooperates internationally through INTERPOL. The assessment team has been assured that cooperation has been good and fruitful. However, no statistics are available on the amount of information exchanges with regard to ML/TF through Interpol.

CED

[66] The GSC has concluded formal information sharing agreements with the following countries: Denmark – November 2011; Malta – August 2012; Estonia – May 2013; UK – July 2013; Jersey – June 2014; Alderney – October 2014; Seychelles – April 2016. The GSC has also signed a letter of intention with the Netherlands in May 2015. The information sharing agreement with the UK is the most actively used arrangement. This is because the UK market is a large gambling market and many IoM licensees are active in that market. The GSC has also approached other gambling authorities for information sharing MOUs since 2009 and the approach has been declined by those countries.

562. The CED cooperates closely with their UK counterparts, i.e. HMRC and the UK Border Force, especially where competences are shared, such as the import/export of potential dual-use goods, day to day customs, excise and VAT matters.

563. Whilst MLA requests are routed via AGC, mutual administrative assistance in customs and indirect taxation, import and export controls and trade controls on the trafficking and brokering of weapons and other sensitive goods, as well as UN/EU sanctions, including where criminal activity might be involved, takes place with - HMRC; UK Border Force; the UK National Crime Agency; VAT and customs authorities in other Member States; customs attaches in London embassies and high commissions; the UK Export Control Organisation; and with the UK Foreign and Commonwealth Office and HM Treasury in respect of UN/EU sanctions. In the 5 years to 2016, the CED handled 194 mutual administrative assistance requests, with 134 dealt with by its Law Enforcement Section because of a suspicion of fiscal fraud or other illegal activity. The Law Enforcement Section also undertook 11 investigation cases which related to mutual assistance request.

ITD

564. The IoM is viewed by its key information exchange partners as a highly respected, efficient and effective member of the Global Forum on Transparency and Exchange of Information for Tax Purposes (OECD). Global Forum members are subject to a peer review process and, following its 2011 peer review report, the IoM is one of only 22 Global Forum Members from the 94 reviewed to date to receive the top 'compliant' rating. The IoM is also among the first countries to implement international standards on automatic exchange of information under the EU Savings Directive FATCA and will in 2017 commence automatic exchange of information under the CRS.

Providing other forms international cooperation for AML/CTF purposes

GSC

565. The evaluation team was advised of many cases where the GSC has successfully requested and provided information for supervisory purposes. 3 of the 22 requests received since 2013 were refused. One was refused due to insufficient information and justification for the request. The GSC sought further information in order to be able to accept the request but it was not provided.

Case Study
The GSC was approached by the regulator from a jurisdiction which had developed a suspicion that a player was cheating with a view to defrauding a company licensed in that jurisdiction. The request sought to identify whether a similar typology had been detected with IoM licensees. The GSC conducted a survey and discovered that such activity had indeed been detected. The GSC advised the foreign regulator that information did exist which would be helpful and advised him to approach the IoM formally through the FCU.

IOMFSA

566. Most of the exchange of information requests handled by IOMFSA relate to the fit and proper status of individuals or regulated persons. Routine regulator to regulator requests are typically handled by the Supervision, Insurance and Pensions Divisions and Authorisations teams, although they may also come through Enforcement as a SIS request. Exceptionally there may be correspondence over a particular problem such as a potential fraud in which the IOMFSA has corresponded with regulators in the USA, Cayman Islands, Channel Islands, Malta, Gibraltar and the UK.

567. In the period 2008 to date the IOMFSA has received 52 overseas requests for assistance from MOU signatories. 3 of those could not be satisfied as they were seeking information outside of the IOMFSA's remit and powers. Of the remainder all but 1 of the requests was dealt with in full (or contact was made with the requesting jurisdiction for additional information to clear up anomalies) within the internal benchmark period of 31 days. There has only been one case where assistance

could not be provided. This was because the information gathering powers of the IOMFSA were not appropriate to the reason that the information sought. The relevant powers were available to another authority (HM Attorney General's Chambers) and notwithstanding the lack of statutory powers the staff of the (then) FSC held dialogue with the requesting authority to ensure that the request was redirected to the appropriate IoM authority and to provide all (non- statutory) assistance in ensuring that authority was in a position to assist without undue delay. The request was then satisfied in an effective manner. Also in the period 2008 to date 1,475 referrals were received from members of the regulatory and law enforcement forum and checked against local indices. Wherever relevant local information was identified details were shared with the source of the referral.

FCU

568. As indicated above, no statistics are available on the amount of information exchanges with regard to ML/TF through Interpol. The authorities, however, have provided several recent case examples where this cooperation was actually sought.

The most recent intelligence disseminated back to Interpol in respect of an on-going investigation in country A related to intelligence from a local online gambling authority that identified a target on the Interpol website had been using their gaming platform. The FCU undertook enquiries locally to ascertain the IP address and account details which were held in country B along with another associate identified on line. This intelligence was collated and disseminated back through Interpol to the country A authorities.

ITD

569. The ITD provides constructive information assistance to its overseas partners. This is evidenced by the statistics provided to the evaluation team. During the period from the April 2010 to March 2015, 398 requests for information were received by the IoM. No requests were declined, while 54 requests were withdrawn by the Treaty partners and 333 requests were dealt in full.

International exchange of basic and beneficial ownership information of legal persons and arrangements

570. The authorities respond to foreign requests for co-operation in identifying and exchanging basic and beneficial ownership information of legal persons and arrangements. With regard to beneficial ownership, witnesses from TCSPs are commonly summoned to court to give evidence, answer questions and produce documentation in relation to beneficial ownership, as described above in the MLA section.

	Total	Total Requests re Beneficial Ownership	Requests Regarding Beneficial Ownership					
			Banks	CSP/ TSP	Insurance /Investment	Accountant/Legal	Public Registries	Bank & Other
2010	54	20 (37%)	10	4	0	2	0	4
2011	80	40 (50%)	18	11	0	0	1	10
2012	82	42 (51%)	22	11	2	0	1	6
2013	84	38 (45%)	15	10	1	0	0	12
2014	63	36 (45%)	13	12	0	0	1	11
2015*	50	29 (58%)	17	5	1	0	0	6

*to 18 November 2015

571. Overall, the IoM FIU has received positive feedback from the foreign FIU counterparts on its ability to provide requested information, including information on beneficial ownership of legal persons and legal arrangements. However, some jurisdictions have reported that requests with regard to beneficial ownership had not been responded to by the FIU in a useful manner which has further implications for asset-tracing and the preparation of a formal MLA request. This issue was discussed on-site and the assessment team concluded that this issue derived directly from the FIU`s

former inability to request additional information from reporting entities. However, in the meantime this deficiency appear to resolved as the new FIU Law gives the FIU an additional power to request beneficial information directly from reporting entities, even though its practical impact could not be tested.

572. As for the IOMFSA, out of 52 overseas requests for assistance from MOU signatories, 31 of the requests specifically sought, amongst other things, beneficial ownership information in respect of companies or bank accounts. In all 31 instances this beneficial ownership information was obtained and passed on.

573. The ITD regularly provides information on beneficial ownership to its Treaty partners. Since April 2010 to March 2015, the ITD exchanged BO information in response to 98 information requests.

Conclusion

574. **The IoM has achieved a substantial level of effectiveness for IO.2.**

TECHNICAL COMPLIANCE ANNEX

1. This annex provides detailed analysis of the level of compliance with the FATF 40 Recommendations in their numerological order. It does not include descriptive text on the country situation or risks, and is limited to the analysis of technical criteria for each Recommendation. It should be read in conjunction with the Mutual Evaluation Report.

2. Where both the FATF requirements and national laws or regulations remain the same, this report refers to analysis conducted as part of the previous Mutual Evaluation in 2009. This report is available from http://www.coe.int/t/dghl/monitoring/moneyval/Countries/Isle_of_Man_en.asp.

Recommendation 1 - Assessing Risks and applying a Risk-Based Approach

3. At the time of the 2009 MER, there was no requirement to conduct a national risk assessment or other risk-related requirements set out in R.1.

4. *Criterion 1.1* (Met) - The IoM conducted its first NRA in 2014/2015 with a view to identifying and assessing its ML/FT risks. The exercise was led by a working group comprising senior officials from various authorities with AML/CFT competences. The working group was formally designated by the IoM Government's Council of Ministers as the NRA Working Group. The World Bank NRA Self-Assessment Tool was used to conduct the exercise. The NRA involved close coordination amongst all the relevant agencies and industry representatives. Multiple sources of information were consulted. Seven thematic working groups were established to collect data and to give consideration to threats and vulnerabilities. These working groups focussed on the following topics: national level threats; national level vulnerabilities; banking, securities, insurance and pensions, other FIs, including money service businesses and foreign exchange, and DNFBPs. The conclusions of the NRA are reasonable.

5. *Criterion 1.2* (Met) - An NRA Working Group was established in October 2013 by the AML/CFT Strategic Group to take forward the work required in respect of the NRA. In October 2014, an NRA Project Manager was appointed to lead and coordinate the work required. This permanent role is established centrally, within the Cabinet Office.

6. *Criterion 1.3* (Met) - The World Bank NRA Methodology recommends periodic updates to the NRA. Political agreement has been secured to update the NRA regularly, at intervals not exceeding four years. A commitment was made by the Chief Minister, as recorded in the introduction to the NRA, that a regular re-examination of risks will be carried out.

7. *Criterion 1.4* (Met) - The IoM published the NRA and the AML/CFT National Strategy 2016-2018 on the IoM official website.[67] In addition, the IoM authorities have communicated the results of the NRA to competent authorities, FIs, DNFBPs and supervisory regulatory bodies.

8. *Criterion 1.5* (Mostly met) - The NRA was completed one year before the on-site visit. Nevertheless, resources had already been allocated and measures taken to address issues identified in the NRA at both national and sectorial level. For instance, the FIU was completely reformed, after a number of deficiencies were identified. The Cabinet Office started a process to develop an overall Government approach to data collection. Steps were being taken to improve financial crime investigations. At an institutional level, the IOMFSA allocated additional resources to some areas which have been identified as posing a higher risk in the NRA. The GSC adjusted its objectives to focus on higher risk areas. LEAs and the FIU had only just begun to focus their activities in line with the risk profile of the country.

9. *Criterion 1.6* (Partly met) - Part 6 of the AML/CFT Code sets out a number of cases where "simplified CDD measures" may be applied: (i) to "acceptable applicants" (para. 20); (ii) to

[67] https://www.gov.im/about-the-government/offices/cabinet-office/national-risk-assessment/

persons in the regulated sector acting on behalf of a third party (para. 21); (iii) in respect of "generic designated business" (para. 22); and (iv) in respect of insurance business, retirement benefit schemes, collective investment schemes, and the IoM Post office (para. 24). These provisions should more accurately be described as exemptions rather than simplification of measures since they allow nothing to be done rather than something to be simplified, e.g. in line with examples given in the interpretive note to R.10. Accordingly, these exemptions (a number of which are conditional upon certain conditions being met) are assessed here.

10. In the case of "acceptable applicants", a FI is not required to have procedures for verifying the identity of the customer (or its beneficial owners or controllers) where certain conditions apply. It is noted that the concession may be applied to domestic firms of lawyers and accountants, notwithstanding the very recent introduction of a registration regime through the DBRO Act[68].

11. In the case of "persons in the regulated sector acting on behalf of a third party", certain FIs are not required to identify and verify the identity of any person on whose behalf a customer is acting where the customer is a person listed in the AML/CFT Code and strict conditions are met, for example detailed written terms of business and annual testing of compliance therewith. It is noted that this exemption may be applied to accounts operated for: (i) lawyers and accountants in the IoM notwithstanding the very recent introduction of a registration and oversight regime through the DBRO Act[69]; (ii) TCSPs in exceptional circumstances where it is "impractical" to establish a separate designated account, e.g. to hold fees taken in advance or where small operating balances are held by a number of trusts where disproportionate bank charges would otherwise erode balances held; and (iii) online gambling operators.

12. In the case of "generic designated business", DNFBPs are not required to have procedures for verifying the identity of the customer where certain conditions apply and they do not participate in any financial transactions on behalf of their customer, e.g. professional advice or audit services.

13. FIs and DNFBPs are not permitted to apply the above exemptions if: (i) any suspicious activity has been identified; or (ii) where the customer has been assessed as posing a higher risk of ML/TF (except for persons in a regulated sector acting on behalf of a third party).

14. The evaluators do not consider that there is a proven low risk of ML/TF in the case of: (i) acceptable applicants - since it may be applied to lawyers and accountants that are not members of professional self-regulatory bodies and which have only very recently registered under the DBRO Act; and (ii) persons in the regulated sector acting on behalf of a third party – since the exemption may still be applied where a customer acting on behalf of a third party has been assessed as posing a higher risk of ML/TF.

15. As highlighted above, certain elements of CDD can be exempted in business relationships with collective investment schemes. This is considered further under c.24.6 and c.25.1.

16. "Peer to peer" payments are exempted from CDD requirements under the Online Gambling Code where certain conditions are met. Again, the evaluators do not consider that there is a proven low risk of ML/TF since the conditions referred to are not linked to ML/TF risk.

17. It should also be noted that the current AML/CFT Code came into force before the IoM's NRA was completed and that para. 20, 21, 22 and 24 have not yet been updated (as appropriate) to take account of risks identified.

18. *Criterion 1.7* (Partly met) - The NRA was completed not long before the on-site visit and the AML/CFT regime had not yet been tailored entirely to fit the risks identified by either requiring

[68] Many (but not all) firms of advocates, legal registered practitioners and accountants are members of professional self-regulatory bodies that have overseen members for compliance with the AML/CFT Code.

[69] However, a number of such firms of advocates, legal registered practiotioners and accountants were members of professional self-regulatory bodies.

FIs and DNFBPs to take enhanced measures to manage and mitigate the risks, or requiring FIs and DNFBPs to incorporate information regarding higher risks identified in the NRA in their own risk assessments. Some new guidance was issued by the IOMFSA to strengthen or address certain higher risk areas (e.g. trade-based ML).

19. *Criterion 1.8* (Mostly met) - FIs and DNFBPs are permitted to apply simplified CDD in exceptional circumstances. Thus its application is very restricted. However, there is no guidance explaining what constitutes exceptional circumstances.

20. *Criterion 1.9* (Met) - FIs and DNFBPs are supervised for AML/CFT purposes by their relevant regulatory body (see analyses to Recs. 26 and 28 for details). As part of their regulatory remit these bodies monitor compliance of the FI or DNFBP with all of the AML/CFT obligations currently imposed on that FI or DNFBP and take appropriate action where compliance is less than satisfactory.

21. *Criterion 1.10* (Met) - FIs and DNFBPs are required to identify, assess and understand the ML/TF risks in relation to their business, customers and technological developments (paras. 6, 7 and 8 of the AML/CFT Code, and the IAMLR). The business risk assessment must be documented in order to demonstrate its basis and conclusions. This enables FIs and DNFBPs to provide risk assessment information to the supervisory authorities. The risk assessment must be undertaken as soon as reasonably practicable after the person commences business. It must be regularly reviewed and, if appropriate, amended so as to keep it up-to-date. All relevant risk factors must be taken into account[70] before determining the level of overall risk and the appropriate level of mitigation to be applied. Similar provisions are in place regarding customer risks (para. 7(2)(a) of the AML/CFT Code) with the exception that a customer risk assessment must be undertaken prior to establishment of a business relationship or the carrying out of an occasional transaction with or for that customer.

22. The Online Gambling Code anticipates the risks inherent in online gambling, so a risk assessment is only required for customers rather than a broader assessment of risks across a large variety of products with different characteristics. In addition, guidance has been issued by the GSC, which provides additional clarity on the requirements and expectations regarding the risk-based approach. There is a mechanism in place for risk assessment information to be provided to the GSC.

23. *Criterion 1.11* (Met) - FIs and DNFBPs are required to have procedures and controls, which are approved by senior management, to enable them to manage and mitigate the risks that have been identified by risk assessments (sub-paras. 4(2) and 4(3) of the AML/CFT Code, Reg. 26(8) of the IAMLR and para. 4 of the Online Gambling Code). There is also a requirement to monitor the implementation of those controls (para. 29 of the AML/CFT Code, Reg. 36 of the IAMLR and para. 21 of the Online Gambling Code) and to take enhanced measures to manage and mitigate risks where higher risks are identified (para. 15 of the AML/CFT Code, Reg. 13(2) of the IAMLR and para. 6(3) of the Online Gambling Code).

24. *Criterion 1.12* (Mostly met) - The IoM has extended the exemptions provided for under the FATF standards in the AML/CFT Code and Online Gambling Code, although without demonstrating low risk or that the pre-conditions under the standard have been met. Simplified measures and exemptions may not be availed of where a FI or DNFBP has identified suspicious activity.

Weighting and Conclusion

[70] Para. 6(3) of the Code: (a) the nature, scale and complexity of the person's activities; (b) the products and services provided by the person; (c) the persons to whom and the manner in which the products and services are provided; (d) reliance on third parties for elements of the customer due diligence process; and (e) technological developments.

25. The IoM meets c.1.1 to 1.4, and 1.9 to 1.11. It mostly meets c.1.5, 1.8 and 1.12 and partly meets c.1.6 and 1.7. **R.1 is rated largely compliant**.

Recommendation 2 - National Cooperation and Coordination

26. In the 2009 Report, the IoM was found compliant with R.31.

27. *Criterion 2.1* (Met) - The IoM has AML/CFT policies which are informed by ML/TF risks, and has formulated an action plan that addresses the findings of the recently completed NRA. The NRA has identified a significant number of national and sectorial actions, some of which have already informed policy and legislation (e.g. the development and introduction of two acts regarding terrorism and the FIU). Further changes arising out of the NRA are being introduced at regulatory and national level. The NRA also identified the need for a national AML/CFT Strategy to be developed which will support the commitment of the authorities and identify ways in which that commitment can be delivered. The IoM has published the NRA and the AML/CFT National Strategy 2016-2018.[71] The strategy provides a framework for overall monitoring purposes, with the strategic goals reflecting the key areas for action identified in the NRA.

28. *Criterion 2.2* (Met) - The IoM Council of Ministers is the highest level decision-making body within the IoM. It has the ultimate authority for setting national and international AML/CFT policy. In matters relating to AML/CFT, the Council of Ministers is advised by the Chief Secretary who is the Chair of the AML/CFT Strategic Group, which is in turn advised by a Technical Group.

29. *Criterion 2.3* (Met) - As mentioned under R.1, the AML/CFT Strategic Group is chaired by the Chief Secretary and includes representatives of several key agencies. Also a number of statutory gateways and working groups exist, which allow co-operation and the sharing of information between law enforcement and regulatory bodies in the IoM.

30. Mechanisms are in place enabling policy makers, the FIU, law enforcement and other competent authorities, including regulators, to co-operate and where appropriate co-ordinate domestically with regard to the implementation of policies and activities to combat ML, also with respect to information sharing. A key factor in such co-operation is the existence of the relevant statutory gateways. These mechanisms apply at both policy-making and operational levels.

31. *Criterion 2.4* (Met) - The co-operation and co-ordination mechanisms for combating ML/FT are also utilised for combating the financing of proliferation of weapons of mass destruction. Development and implementation of policies and activities to combat proliferation is co-ordinated through the AML/CFT Technical and Strategic Groups. Members from other agencies, including intelligence services, can also be invited by the AML/CFT Strategic Group Chair.

Weighting and Conclusion

32. The IoM meets all criteria. **R.2 is rated compliant**.

Recommendation 3 - Money laundering offence

33. In the 2009 Report, the IoM was rated partially compliant for these requirements (paras. 116-177). The factors underlying the rating for R.1 were: 1) the restrictive purpose requirement for the ML acts of converting and transferring, concealing or disguising of proceeds of crime; 2) the defences (payment of adequate consideration) which were considered to be beyond the standards provided for by Vienna and Palermo Conventions; 3) the ML offence based on TF did not fulfil all the material elements of the international standards; 4) self-laundering was not covered by the ML acts of acquisition, possession or use, and by the ML offence based on TF. The factors underlying the LC rating for R.2 related to the effectiveness of the sanctioning regime and on the stand-alone ML offence, which fall outside the scope of the present analysis.

[71] https://www.gov.im/about-the-government/offices/cabinet-office/national-risk-assessment/

34. At the time of the 2009 Report, the ML offences were covered by the provisions of the CJA 1990, DTA 1996 and ATCA. The first two acts were repealed and replaced by the POCA 2008 (in force since August 2009). ATCA provisions remain in force, though they were amended in 2011.

35. *Criterion 3.1* (Met) - Under the POCA 2008, the restrictive purpose requirement "of avoiding prosecution for predicate offence" with regard to ML acts of "concealing or disguising" and "converting or transferring", was excluded (sec. 139). The defence (payment of adequate consideration) in relation to the acquisition, possession, or use of criminal proceeds was excluded - sec. 141(6) repealed. Under the new provisions of the POCA 2008 and the amendments introduced to ATCA, self-laundering is covered now for both ML offences i.e. ML offence (including ML acts of acquisition, possession or use) and ML offence in relation to TF (sec. 141 of the POCA 2008 and sec. 10 of the ATCA). The existence of an arrangement (written, oral, or implied) is not required by the ML offence related to TF due to the subsequent legislative amendments of 2011. It is sufficient that the person "facilitates the retention or control of the terrorist property" (sec. 10 of the ATCA). Therefore, the ML offence under the IoM law covers all the material elements required by the Palermo and Vienna Conventions.

36. *Criterion 3.2 and 3.3* (Met) - The ML offence is defined in relation to criminal property obtained from criminal conduct. Criminal conduct is: a) an offence in IoM; b) would constitute an offence if it occurred in IoM (sec. 196 of the POCA 2008). Thus, any offence can be a predicate offence for ML. The 2009 report concluded that all designated categories of offences are covered under IoM law (see para. 141). Tax crimes are also covered.

37. *Criterion 3.4* (Met) - The ML offence extends to any type of property. There is also no minimum or maximum value established. "Criminal property" is a) the benefit from criminal conduct, in whole or in part, obtained directly or indirectly; b) property which the defender knows or suspects is or represents such benefit (sec. 158(3) of the POCA 2008). The definition of property is wide enough to fulfil the standard. It is considered to cover "all property wherever situated" and includes: money; all forms of real or personal property; and things in action and other intangible or incorporeal property (sec. 132 of the POCA 2008). "Terrorist property" and "property" under the ATCA are also defined broadly enough to meet the standard's requirement (secs. 6 and 75 of ATCA) (see paras. 134 and 135 of the 2009 Report).

38. *Criterion 3.5* (Met) - The ML offence does not require a conviction for the predicate offence. Thus, there are no legislative barriers to autonomous ML prosecutions/ convictions. It must be proved, beyond reasonable doubt, that the property constitutes proceeds of crime and that the defendant has committed the alleged laundering offence.

39. *Criterion 3.6* (Met) - The provisions of the ML offences regulated by the (repealed) CJA 1990 and DTA 1996 norms covered the criminal conduct committed abroad (that would have constituted a predicate offence had it occurred in IoM) – para. 146 of the 2009 Report. The same approach is maintained by the ML offence provided by POCA 2008. A criminal conduct is considered to be conduct which: a) constitutes an offence in IoM; or b) would constitute an offence if occurred in IoM (sec. 158(2) of the POCA 2008). The ML offence provides for an exemption with regard to foreign conduct. Where a person knows, or believes on reasonable grounds, that the relevant foreign criminal conduct was not, at the time it occurred, an unlawful conduct in that country/territory, the ML offence is not considered to be committed. Such an exemption can be limited by an order of the Department of Home Affairs (DHA) which prescribes criminal conduct by description as exempt from this exclusion. In case of a conduct prescribed by the order, the liability for ML would remain whether or not the conduct was unlawful (sec. 139-141). Order 2013 (SD 322/13) – exceptions to overseas conduct defence order – prescribes certain criminal conduct in respect of offences committed under sec. 139-141, para. (3)(b)(ii) of the POCA 2008.

40. *Criterion 3.7* (Met) - The ML offences of concealing, disguising, converting and transferring, removing of criminal property (sec. 139) and of acquisition, use and possession of criminal

property (sec. 141) apply to both the predicate offender or a third party. Arrangements under sec. 140 apply to a person who enters into an arrangement with the predicate offender. Thus, the new provisions of the ML offence remedy the deficiencies with regard to self-laundering offence identified by the previous assessment (for the offences of acquisition, possession or use). ML offences related to the TF predicate offence regulated by ATCA were considered by the previous assessment not to cover self-laundering. The 2011 amendments prescribe the offence in relation to "a person", thus extending it to self-laundering.

41. *Criterion 3.8* (Met) - The ML offence applies also to property which the defendant knew or suspected that it is or represented benefit from criminal conduct. Thus, the criminal property, for the purpose of ML offence, is also defined by the state of mind of the accused. There was no jurisprudence at the time of the previous assessment to prove that the intent and knowledge could be inferred from objective factual circumstances, but it was recognised that the English common law principle regarding the ability to make reasonable inferences from objective factual circumstances would apply. The IoM authorities presented case-law confirming judicial practice. Accordingly, the prosecution may prove that the property derives from criminal conduct 1) either by evidence showing that it derived from a specific crime; or 2) by evidence from which the jury is entitled to infer that the property can be derived from crime ("an irresistible inference") – Anwoir, Elmoghrabi, Meghrabi, Mclntosh [2008].

42. *Criterion 3.9* (Met) - The sanctions provided by the ML offence under the POCA 2008 are similar to those prescribed by the previous CJA 1990 and DTA 1996 provisions. The last assessment concluded that the sanctions for ML seemed to be in line with other serious crimes under IoM law and that, overall, they seemed to be proportionate and dissuasive.

43. *Criterion 3.10* (Met) - Corporate criminal liability applies to the ML offence – sec. 221 of the POCA 2008, Offences by bodies corporate. Criminal liability for ML offences related to TF predicate offences under ATCA is also applicable for legal persons. It refers to "a person" who, according to the Interpretation act 1976, includes anybody of persons, corporate or unincorporated. Parallel civil proceeding could also be brought against the legal person. Corporate criminal liability does not prejudice the criminal liability of a natural person.

44. Civil proceedings could be brought against the officers for disqualification as persons unfit to hold corporate office pursuant to sec. 4 of the Company Officers (Disqualification) Act 2009, previously sec. 26 of the Companies Act 1992. The disqualification powers under Company Officers (Disqualification) Act 2009 may be used in addition to or as an alternative to criminal sanction. The disciplinary powers of the IOMFSA set out under R. 35 may also be used in addition to or as an alternative to criminal sanction.

45. *Criterion 3.11* (Met) - IoM law allows for the prosecution of all parties that may be involved in the commission of the ML offence. The attempt, conspiracy or incitement to commit, aiding, abetting, counselling or procuring the commission of a ML act are covered by letter (b) and (c) sec. 158(11) of the POCA 2008. These conducts are also provided by the ML offence under sec. 198 of the POCA 2008, which applies as well to ML acts in relation to a TF predicate offence (of the sec. 10 of the ATCA). Failure to disclosure/tipping off is an ancillary ML offence under sec. 198A. An attempt, conspiracy or incitement, aiding, abetting, counselling or procuring the commission of disclosure/ tipping off are also ancillary ML offences under sec. 198A. It also applies to Disclosure of information: duty and Failure to disclose under sec. 11 and 14 of the ATCA. Conspiracy, inciting, attempting, aiding, abetting, counselling or procuring of ML of terrorist funds is also provided for by sec. 13 of ATCA.

Weighting and conclusion

46. The IoM meets all the criteria. **R.3 is rated compliant**.

Recommendation 4 - Confiscation and provisional measures

47. In the 2009 Report, the IoM was rated partially compliant with the then R.3 of the FATF Recommendations. While R.4 in the 2012 version of the Recommendations is substantially similar, some modifications were introduced. The shortcomings included: 1) the narrower scope of the criminal confiscation due to the deficiencies in ML and TF criminalisation; 2) concerns with regard to the possibility to confiscate laundered property in stand-alone ML cases; 3) no equivalent value seizure measures before start of the proceeding; 4) barriers to application of equivalent value confiscation and seizure for TF. Due to subsequent legislative amendments which entered into force after the assessment (Part 2 POCA 2008 in force since 2009 and ATC 2011 amendments to ATCA), the last two deficiencies were remedied as described below.

48. *Criterion 4.1* (Mostly met) - POCA 2008, ATCA and CLA 1981 represent the legal framework enabling the confiscation and restraint measures in IoM. Part 2 of POCA 2008 covers confiscation and restraint in respect of all crimes, except those covered by ATCA connected to terrorism offences. CLA 1981 enables the confiscation of instrumentalities in respect of all crimes, while the confiscation of instrumentalities related to terrorism offences is also regulated separately by ATCA.

49. Before August 2009, when the new amendments to POCA entered into force, there were four acts governing the confiscation measures: CJA 1990, DTA 1996, ATCA and CLA 1981. POCA 2008 consolidated and replaced separate drug trafficking and criminal justice legislation, while the specific ATCA and CLA 1981 provisions remain applicable. This specification has the purpose to highlight that the 2009 Report focused on the CJA 1990 and DTA 1996 provisions (which were repealed), ATCA and CLA 1981 provisions (still in force) and POCA 2008 (Part 1 on civil recovery procedure, in force before the on-site visit, since October 2008 and Part 2 on confiscation and restraint, in force after the on-site visit, since August 2009).

50. The description of the structure and the areas covered by Part 2 of the POCA 2008 under para. 226 of the 2009 Report remains valid and will not be repeated. However, two important aspects of the Act are worth emphasising here: (i) the criminal lifestyle assumption when dealing with confiscation orders, where the particular criminal conduct will be considered only in the absence of the former; and (ii) the civil recovery procedure.

51. (a) (Mostly met) - With respect to the confiscation of "laundered property", the situation remains mainly unchanged since the previous assessment. The absence of general provision explicitly covering the confiscation of the laundered assets as the object of the (autonomous) ML offence ("corpus delicti") in a stand-alone prosecution was identified as a deficiency in the previous MER (see para. 214). The conclusion of the previous assessment was that the relevant legal provisions of POCA 2008, CJA 1990 and the DTA 1996 need to be tested in stand-alone ML prosecutions or confirmed in authoritative doctrine, in order to ensure that the confiscation of laundered assets is applied. According to the 2013 IoM Progress Report, the jurisprudence is only being developed.

52. (b) (Met) - As stated in the 2009 Report (para. 228 in relation to the repealed confiscation regime under CJA 1990 and DTA 1996), the confiscation is value-based and criminal proceeds are not subject to confiscation as such. This remains valid for the new provisions of POCA 2008, which replaced the mentioned acts. The central focus is on "benefit" from the criminal conduct which is the "property" or "any pecuniary advantage" obtained as a result of or in connection with the conduct (sec. 124(4) and (5)). The property and the pecuniary advantage are considered to be obtained even if they are not connected with the criminal conduct but have some other connection (sec. 124(6)). The defendant's benefit is the value of the property obtained (sec. 124(7)). The calculation of the value of the benefits obtained from criminal conduct would include substitute assets and any pecuniary advantage.

53. The confiscation of instrumentalities used, which facilitated or intended to be used for the commission of an offence is covered by sec. 16 of CLA 1981. It applies to all categories of offences, including terrorism. Besides, the special provisions of the ATCA also can be used for the confiscation (forfeiture) of instrumentalities relating to terrorism as it is described below.

54. (c) (Met) - Sec. 16 of the ATCA enables the forfeiture of "any money or other property" related to terrorism offences. The forfeiture orders can be made under the conditions that the defendant is convicted for terrorism offences (sec. 7-10 of ATCA) and that the money or other property, at the time of the offence, were in the possession or under the control of the defendant. The court may order the forfeiture of the money or other property which a) had been used for the purposes of terrorism b) intended to be used for such purposes c) where the defendant knew or had reasonable cause to suspect that it would or might be used for those purposes. Payments and rewards received wholly or partly, directly or indirectly in connection with the commission of the terrorism offences are also subject to forfeiture under sec. 16(7).

55. (d) (Met) - The confiscation under POCA 2008 is value based. It relates to the "benefits" from the general or particular criminal conduct (sec. 66(4)) and the "recoverable amount" as decided by the court (sec. 66(5)). The new provisions of POCA 2008 remedy the concerns of the previous assessment in relation to the equivalent value seizure (paras. 238 and 253 of the 2009 Report). Still, the equivalent value seizure is not possible to be made under the Police Powers and Procedures Act (1998) (PPPA 1998) (para. 233) as this issue has not been addressed by any subsequent amendments to PPPA 1998. At the time of the previous evaluation, ATCA did not provided for the corresponding value forfeiture. The 2011 amendments – Special forfeiture orders under sec. 16B remedy the shortcoming by enabling the forfeiture of money or other property which are not related to the offence "up to the equivalent value of the money or other property mentioned in sec. 16 or 16A" – (16B(1c) and (2)).

56. *Criterion 4.2* (Met) - POCA 2008, ATCA, PPPA 1998 and CJA 1990 constitute the legal bases allowing the use of investigative powers. The new provisions of POCA 2008 on production orders replaced the correspondent provisions of the CJA 1990 and DTA 1996. Nevertheless, the powers related to search of premises and the special investigative powers of AG for "serious or complex cases" as described in the 2009 Report (paras. 242 and 243) were not affected and remain valid (secs. 11 and 12 of PPPA 1998 and sec. 24 of CJA 1990). For the purpose of confiscation or civil recovery investigation, detained cash or ML investigation, POCA 2008 (Part 4) provides for a variety of investigative powers for identifying and tracing the property: production orders (sec. 163), disclosure orders (sec. 174), customer information orders (sec. 180) and account monitoring orders (sec. 187). For the TF investigations, ATCA provides for account monitoring orders (sec. 18 and Schedule 4), warrant for entering and searching the premises (sec. 24 and Schedule 5) and customer information orders (sec. 25 and Schedule 6).

57. Provisional measures to preserve the property subject to confiscation are provided by PPPA 1998, POCA 2008 and ATCA. They comprise: the general power to seizure as described by para. 233 of the 2009 Report (sec. 22 of PPPA 1998), restraint orders (sec. 96-102 of POCA 2008, which replaced the correspondent provisions of the CJA 1990 and DTA 1996) and special procedure for seizure and detention of "terrorist cash" or restraint orders under ATCA (Schedule 3, part 2 (2) and Schedule 2.5 (1) and (2)). The restraint order may be made ex-parte under POCA (sec. 98) and in private without prior notice under ATCA (Schedule 2.5(4)). Unlike the previous restraint orders under DTA 1996 and CJA 1990, the restraint orders under 2008 POCA provisions can be made during both criminal investigation and criminal proceeding.

58. The previous evaluation concluded that the IoM legislation ensures adequate powers to void actions that are intended to obstruct effective confiscation or would undermine the value of realizable property (para. 250).

59. *Criterion 4.3* (Met) - The 2009 Report concluded that the criterion on the protection of bona fide third party (the former c. 3.5) is met (see paras. 245-249) and therefore, in the absence of any subsequent legislative changes on this matter, the conclusion remains valid.

60. *Criterion 4.4* (Partly met) - POCA 2008 establishes certain powers related to property management for the receiver (sec. 14(1) Schedule 1) and the trustee, for civil recovery, (sec. 23(6) Schedule 2). They include (a) selling or otherwise disposing of assets comprised in the property which are perishable or which ought to be disposed of before their value diminishes; (b) carrying on, or arranging for another to carry on, the trade or the business; (c) incurring capital expenditure in respect of the property. Arguably, these powers are also applicable in relation to the instrumentalities and the money or property frozen, seized or confiscated under the CLA 1981 and ATCA as amended. There are no express provisions enabling similar powers under these two acts. In that respect, the IoM authorities indicated that the POCA 2008 provisions would be applicable as it was widely drawn in order to include any "property obtained through unlawful conduct". Such an interpretation, of course, would need to be endorsed by the actual practice. The court may appoint a receiver if the property requires management. Nevertheless, as indicated by the authorities, the practice is that the goods, other than cash, are left in situation, under the responsibility of the offender.

61. Beside these powers, there seems to be no framework for managing and overseeing the management of frozen, seized and confiscated property: a designated authority responsible for preserving and managing the property; sufficient resources to handle all aspects of the asset management (because of the maintenance and service cost the goods are left with the defendant); a mechanism ensuring the transparency and assessing the effectiveness of the system, etc.

62. All confiscated money and the funds derived from sale of confiscated property are placed into the Seized Assets Fund, managed by the Treasury. The fund can be used for countering the effects of criminal activities, especially serious and organised crime; for promotion and implementation of community safety initiatives and those designed to counter the effects of drugs and alcohol; as well as for the initiatives related to emerging threats and developing issues (as defined by the Strategic Tasking and Co-ordinating Group of the Constabulary).

Weighting and conclusion

63. The IoM has a solid legal framework for confiscation but does not have measures in place to manage seized or confiscated property. The confiscation of laundered property is not explicitly covered. **R.4 is rated largely compliant.**

Recommendation 5 - Terrorist financing offence

64. In the 2009 Report, the IoM was rated largely compliant with former SR.II. The assessors found that the FT offence did not contain a reference to international organisations and the definition of "terrorism" did not extend to all terrorism offences as defined in the nine Conventions and Protocols listed in the Annex to the TF Convention.

65. *Criterion 5.1* (Met) - The FT offence is consistent with Art. 2 of the International Convention of the Suppression of the Financing of Terrorism. The amendments to the ATCA addressed the deficiencies identified in the 2009 Report.

66. *Criterion 5.2* (Mostly met) - FT is criminalised under sec. 7 – 10 of ATCA 2003. There are 3 main FT offences: Fund Raising (sec. 7); Use and Possession (sec. 8); and Facilitating Funding (sec. 9). Under the amended sec. 10, a person commits an offence of ML (ML of terrorist property) if he facilitates the retention or control of terrorist property (of which the definition includes 'money or other property which is likely to be used for the purposes of terrorism, including any resources of a proscribed organisation'), by concealment, disguise, conversion, removal from the jurisdiction, transfer to nominees or in any other way.

67. The offences of *Fund Raising* and *Use and Possession* applies a subjective test of whether an individual intended or had reasonable cause to suspect that property may be used for the purposes of terrorism. The offence of *Facilitating Funding* applies a subjective test of whether an individual had knowledge or reasonable cause to suspect or failed to exercise due diligence as to whether funds will or may be used for the purposes of terrorism. Terrorism is broadly defined in sec. 1 to include terrorist acts and action taken for the benefit of proscribed organisations. The FT offences do not criminalise the intentional financing of individual terrorists for purposes other than their use for terrorist acts. The criminalisation of the intentional financing of terrorist organisations for purposes other than their use for terrorist acts is limited to proscribed organisations (Part II of ATCA provides the list of proscribed organisations). The IoM legislation uses the concept of recklessness to criminalise the financing of an individual terrorist or an unproscribed terrorist organisation in the absence of a link to a specific terrorist act or acts. However, the offences do not criminalise the funding of unproscribed terrorist organisations for legitimate purposes (e.g. humanitarian aid). According to FATF Guidance on R.5 (para. 29) the criminalisation of recklessness as to the use of funds or other assets for terrorist purposes could be considered as consistent with the requirement in some circumstances, although it cannot substitute for the criminalisation of the intentional financing of a terrorist organisation.

68. *Criterion 5.2bis* (Met) - The IoM considers that these conducts would be covered by sec. 7 (3), 9 and 46B of ATCA, which criminalises the provision of property to persons for the purposes of terrorism. However, it must be noted that this interpretation is not yet confirmed by relevant jurisprudence and giving the importance of this particular issue the assessment team recommends the IoM to give consideration to introducing relevant specific explicit provisions.

69. *Criterion 5.3* (Met) - The FT offence applies to all funds, whether from a legitimate or illegitimate source (sec. 7 – 10 of ATCA refer to "money or other property". "Property" is defined in sec. 75).

70. *Criterion 5.4* (Met) – The FT offences do not require that the funds are actually used to carry out or attempt a terrorist act(s) or be linked to a specific terrorist act. .

71. *Criterion 5.5* (Met) - As general principle of English Common Law, the intent and knowledge required to prove the offence can be inferred from objective factual circumstances. There is still no jurisprudence on the FT offence available (see IO 9), but, as described under c.3.8, the IoM authorities have provided case-law proving compliance with the criterion in the context of ML.

72. *Criterion 5.6* (Met) - FT is punishable with a maximum penalty of 14 years' imprisonment and a fine for natural persons.

73. *Criterion 5.7* (Met) - Legal persons may be liable for the FT offence under sec. 1(4)(b) of the ATCA and in accordance with sec. 3 of the Interpretation Act 1976, which defines a person as including any body of persons, corporate or unincorporated. When legal persons are subject to criminal liability for terrorist financing, this does not preclude the possibility of parallel criminal, civil or administrative proceedings. For example, criminal proceedings could be brought against the officers of the legal person or civil proceedings could be brought against the officers for disqualification as persons unfit to hold corporate office pursuant to sec. 4 of Company Officers (Disqualification) Act 2009. The disqualification powers under Company Officers (Disqualification) Act 2009 may be used in addition to or as an alternative to criminal sanctions. The disciplinary powers of the IOMFSA set out under R. 35 may also be used in addition to or as an alternative to criminal sanctions. The measures described are without prejudice to the criminal liability of natural persons. ATCA prescribes criminal sanctions for supporting a proscribed organisation (s.4) – imprisonment for 10 years and/or and unlimited fine.

74. *Criterion 5.8* (Met) - There are appropriate ancillary offences to the FT offence, including: participation in; association with or conspiracy to commit; attempt; aiding and abetting; facilitating; and counselling and commission under sec. 139-145 of POCA 2008 and sec. 10, 11 &

14 of ATCA (see C 3.11). Aiding, abetting, counselling or procuring an offence under sec. 7-10 of ATCA is a Convention Offence and as such falls within the definition of terrorism.

75. *Criterion 5.9*. (Met) - FT is designated as a ML predicate offence.

76. *Criterion 5.10* (Met) - The FT offences apply regardless of the geographical location of the person alleged to have committed the offences, the terrorist organisation or the terrorist act (ATCA sec. 1 and 49).

Weighting and Conclusion

77. The IoM meets c.5.1, 5.2*bis*, 5.3, 5.4 and 5.5.-5.10. It mostly meets c.5.2. **R.5 is rated largely compliant**.

Recommendation 6 - Targeted financial sanctions related to terrorism and terrorist financing

78. In the 2009 Report, the IoM was rated partially compliant with the former SR III. The assessors found that there was no procedure in place to respond to and examine foreign freezing requests, the definition of "funds" did not include a reference to 'jointly' and 'indirectly', there was no delisting or unfreezing procedure provided in the context of the EC Regulation lists and no access was provided to assets frozen under UNSCR 1267 for humanitarian reasons and basic expenses. These deficiencies were addressed.

79. The TFS regime of the IoM is dependent on that of the UK, which in turn is subject to the EU TFS framework. The implementation by the UK of UN and EU TFS are extended to the IoM by specific UK orders (para. 259 to 264 of the 2009 Report). However, the IoM enacted the TOCFR in 2014 to strengthen its TFS regime by, for instance, explicitly stating that any designations made by the UK Treasury will have immediate effect in the IoM and giving powers to the IoM Treasury (delegated to the CED) to make its own designations. The TOCFR was amended in 2016 to broaden the definition of a "designated person" to refer to persons or entities designated by the UNSC (whether for terrorism or proliferation purposes). As a result there is no delay between listing by the UN and the implementation of the restrictions in the IoM.

80. *Criterion 6.1* (Met) - Any proposal for designation to the UN Committees would be made by the UK HM Treasury. Criteria 6.1(a) to (e) are implemented by the relevant UK authorities.

a) *Criterion 6.2* (Met) - a) The IoM implements UNSCR 1373 through the TOCFR (Division 2 of TOCFR). There is an IoM government policy to keep its TFS in line with those of the UK. This means that the IoM maintains asset freezing measures against persons and entities pursuant to UNSCR 1373 where they have been designated by the EU or the UK. In the IoM, the CED has the power to make designations and freezing orders. (Division 2, Subdivision 2 (sec. 18 – 23) of TOCFR). Sec. 18 of TOCFR sets out the grounds for designating persons and entities, which are in line with the criteria of UNSCR 1373. The power to issue freezing orders explicitly extends to situations in which the CED receives a request to make a freezing order from a foreign authority (Subdivision 1 of TOCFR).

b) The identification of targets would be carried out in close co-ordination with the relevant UK authorities.

c) At the EU level, the CP 931 Working Party (WP) of the Council of the EU examines and assesses whether the person meets the designation criteria set forth in Common Position 2001/931/CFSP. At IoM level, the CED can issue freezing orders upon request from a foreign authority if it considers it 'appropriate in the circumstances to make the order' (sec. 14). In addition, the CED applies a protocol contained in Sanctions Notice 29, which further deals with the procedures for considering and making freezing orders under the TOCFR. The protocol provides that requests from authorities outside of the IoM must be considered promptly. It also instructs the Treasury to consider whether the request is supported by a sufficient standard of evidence that the proposed person meets the criteria for designation in UNSCR 1373.

d) At EU level, the CP 931 WP applies a "reasonable basis" evidentiary standard of proof for designation decisions, which are not conditional on the existence of criminal proceedings (CP 2001/931/CFSP Art. 1(2) and (4)). In the IoM, the applicable standard of proof for designating persons and entities is 'reasonable suspicion' that a person is involved in terrorist activity (sec. 18 TOCFR). For issuing freezing orders based on foreign request, the CED Protocol as mentioned under c) instructs the Treasury to consider whether the request is supported by a 'sufficient standard of evidence' that the proposed person meets the criteria for designation in UNSCR 1373, and explicitly states that this is not conditional upon the existence of criminal proceedings (point 26 and 27 of the Protocol).

e) Given the constitutional status of the IoM, any such request would of necessity be formally routed to and via the UK authorities. This does not preclude informal, direct contact with the competent authority of any particular country thought to be particularly affected, using powers available for the disclosure of information and documents in sec. 174B of CEMA 1986.

81. *Criterion 6.3* (Met) - a) The IoM Constabulary, the FCU and the CED have legal authority and mechanisms to collect or solicit information to identify persons and entities that, based on reasonable grounds, or a reasonable basis to suspect or believe, meet the criteria for designation. (sec. 19 and 26 and Schedule 5 and 6 of ATCA, sec. 174B to 174D CEMA 1986, Schedule to the European Communities (Terrorism Measures) (Enforcement) Regulations 2008) b) EU-level designations take place without prior notice to the person/entity identified (EC Reg. 1286/2009 preamble para. 5). Under the TOCFR, a person or entity can be designated *ex parte*.

82. *Criterion 6.4* (Met) - TFS are implemented without delay (sec. 3(1)(c) of the TOFCR 2014).

83. *Criterion 6.5* (Mostly met) - The CED has the role of implementing UN and EU sanctions.

a) The TOFCR 2014 ensures that funds or other assets are frozen without delay and without prior notice. Under the EU regulations implementing UNSCRs 1267/1989 and 1988, there is an obligation to freeze all funds, financial assets, or economic resources of designated persons/entities.[72] Under UNSCR 1373, the obligation to freeze all funds/assets of designated persons/entities applies immediately to all EU Member States, and without notice to the designated persons/entities. (EU Reg. 2580/2001 Art. 2(1)(a)). EU internals[73] however are not subject to the freezing measures of Reg. 2580/2001, but are subject to increased police and judicial cooperation among Member States (CP 2001/931/CFSP footnote 1 of Annex 1). This gap could be mitigated by the IoM's powers under the TOCFR, but these have not yet been applied.

b) For UNSCRs 1267/1989 and 1988, the freezing obligation extends to all funds/other assets that belong to, are owned, held or controlled by a designated person/entity. For UNSCR 1373, the freezing obligation does not cover a sufficiently broad range of assets under the EU framework (although subsequent regulations cover a wider range) in EU Reg. 2580/2001 art. 1(a) and art. 2(1)(a). The obligations to freeze the funds or assets of persons and entities to be frozen when acting on behalf of, or at the direction of, designated persons or entities is met by the sec. 1-3 of EU (Al-Qaida Sanctions) Order 2013 and EU (Afghanistan Sanctions) Order 2012, sec. 1-4 of European Communities (Terrorism Measures) Order 2002 and 44 to 49 of the TOCFR.

c) Under EU Reg. 2580/2001 (Art. 2), 881/2002 (Art. 2(2)), 1286/2009 (Art. 1(2)), 753/2011 (Art. 4) and 754/2011 (Art. 1), EU nationals and persons within the EU are prohibited from making funds and other assets available to designated persons and entities. The IoM has additionally applied the relevant requirement by virtue of domestic measures described under c.6.5. a).

d) The mechanism for communicating designations to FIs and DNFBPs is described under IO 10.

[72] EU Regs. 881/2002 Art. 2(1), 1286/2009 Art. 1(2), 753/2011 Art. 4, and 754/2011 Art. 1.
[73] "EU internals" are persons who have their roots, main activities, and objectives within the EU.

e) Natural and legal persons (including FIs/DNFBPs) are required to provide immediately any information about accounts and amounts frozen under domestic legislation per Art. 5.1 of EU (Al-Qaida Sanctions) Order 2013, Art. 8.1 of EU (Afghanistan Sanctions) Order 2012, Art. 4 of European Communities (Terrorism Measures) Order 2002 and sec. 25 and 26 of TOCFR.

f) The rights of *bona fide* third parties are protected (Art. 6 of EC Reg. 881/2002, Art. 7 of EC Reg. 753/2001, Art. 4 of Reg. 2580/2001, sec. 43 of TOCFR).

84. *Criterion 6.6* (Mostly met) - a) The IoM would discuss concerns about continued designations under UNSCR 1267/1988 and 1989 with the authorities in the UK, who would be responsible for submitting de-listing requests to the relevant UN Sanctions Committees.

b) When the EU or UK de-lists a person or entity, the delisting has automatic effect in the IoM and the funds and other assets are unfrozen. If the IoM were to individually designate a person or entity under the TOCFR, designations may be varied or revoked by the CED at any time if this is considered to be appropriate (sec. 21 and 22 TOCFR).

c) At the EU level, designated persons or entities may institute proceedings according to Art. 263 para. 4 and Art. 275 para. 2 TFEU before the Court of Justice of the EU in order to challenge the relevant EU measures, whether they are autonomously adopted by the EU, autonomously adopted by the EU in line with UNSCR 1373 (2001), or based on listings pursuant to UNSCR 1267 (1999). In addition, for persons designated by the CED and for by those affected by either the Al-Qaida and Taliban (UN measures) (IoM) Order 2002, Part 4 of TOCFR provides for appeals against the designation. There is also the common law IoM remedy of Petition of Doleance.

d) & e) At the EU level, there are legal authorities and procedures for de-listing, unfreezing, and allowing a review of the designation by the EC (UNSCR 1267/1989) or the Council of the EU (UNSCR 1988). The designation can also be reviewed using the UN mechanisms of the UN Office of the Ombudsperson (UNSCR 1267/1989 designations) or the UN Focal Point mechanism (UNSCR 1988 designations). These procedures may take place in parallel: Reg. 881/2001 Art. 7a and EU Council Reg. 753/2011 Art. 11. In the EU (Afghanistan Sanctions) Order 2012, persons who wish to submit observations about their listing are advised to do so to the Council of the EU (Art. 11). The "Al-Qaida and Taliban" notice on the website of the CED includes information concerning the availability of the *UN Office of the Ombudsperson.*

f) There are no publicly available procedures to deal with "false positives".

g) Both at the EU and at the IoM level, the communication framework regarding de-listing and unfreezing decisions is the same as described under c.6.5(d). No further guidance is available on obligations to respect de-listing or unfreezing action.

85. *Criterion 6.7* (Met) - At the EU level, there are mechanisms for authorising access to frozen funds or other assets which have been determined to be necessary for basic expenses, the payment of certain types of expenses, or for extraordinary expenses, per Art. 2a of EU Reg. 881/2002, EU Reg. 753/2011, and 5–6 of EU Reg. 2580/2001. In addition, in the TOCFR sec. 50 provides for certain exemptions to the freezing requirements and sec. 51 provides that the Treasury may permit by a licence necessary payments to be made and otherwise authorise access to funds and other assets.

Weighting and Conclusion

86. The IoM meets c.6.1 to 6.4, c.6.7 and it mostly meets c.6.5 and 6.6. **R.6 is rated largely compliant.**

Recommendation 7 – Targeted financial sanctions related to proliferation

87. This recommendation was added to the FATF Standards in 2012. The IoM has, therefore, not previously been assessed against this recommendation.

88. *Criterion 7.1* (Met) - Proliferation-related TFS are implemented through the UK orders, EU TFS regime and the TOCFR. See para. 79.

89. *Criterion 7.2* (Met) - a) See c.6.4.

b) The freezing obligation extends to the full range of funds or other assets required by R.7 (sec. 5A TOCFR).

c) Making available any funds or other assets, other than under a licence (or other narrow exceptions that might be included in an applied EU sanctions Regulation) would be an offence according to the sec. 44 to 49 of the TOCEFR. Where licences are issued, these are granted by the Treasury on the recommendation of the Sanctions Officer at the CED.

d) The mechanism for communicating designations to FIs and DNFBPs is described under IO 10/11.

e) FIs and DNFBPs are obliged to report to CED any assets frozen or actions taken in compliance with the prohibition requirements of the relevant UNSCRs, including attempted transactions (Sanctions Notice 22 para. 14 (b) and 15).

f) The rights of *bona fide* third parties are protected under Art. 42 of EC Reg. 267/2012 and 11 of EC Reg. 329/2007, sec. 43 of TOCFR.

90. *Criterion 7.3* (Mostly met) - The IOMFSA monitors and ensures compliance with R. 7 requirements and has the powers to penalise and sanction where an area of non-compliance is identified (R.26, 27 and 35). The IOMFSA has also direct legal power to test the compliance with sanctions of all the DNFBPs and moneylenders registered under the DBRO Act. The GSC is responsible for monitoring compliance of casinos and online gambling operators (R. 28). The deficiencies identified under the supervisory regime apply under this criterion. Failure to comply with these requirements is punishable by sanctions as described under R. 35.

91. *Criterion 7.4* (Mostly Met)

a) For de-listing the IoM depends on the relevant UK authorities and procedures. Sanctions Notice 26 (which provides general information on sanctions regimes, including those relating to terrorism and proliferation) also includes information on how a person or entity included on the list of those subject to sanctions in the IoM can lodge an appeal to the Sanctions Committee of the UN, may petition that Committee for de-listing by contacting the Office of the Ombudsman at the UN Headquarters in New York; contact the General Secretariat of the Council of the EU for a statement of reasons for their listing by the EU; lodge an appeal in the Court of Justice of the EU; or lodge an appeal against a decision of the Treasury in the High Court under Part 4 of the TOCFR.

b) There is no formal publically known procedure to unfreeze the funds or other assets of persons or entities referred to under this criterion. However, the IoM does not have the power to designate persons under R 7 TFS and relies on the procedures in the UK.

c) Where a sanctions measure includes a specific exemption, such as with basic living expenses (as mentioned in UNSCR 1737 and many EU sanctions Regulations), these would be permitted – with or without the issue of a licence, if required, or confirmation in writing to provide reassurance to the institution or business involved. Schedule 2 to the TOCFR, which sets out requirements for freezing orders for terrorism and proliferation-related purposes, includes a provision for the issue of licences which could or would be used to authorise the use or release of funds where permitted by an exemption.

d) The communication mechanism is described under IO 10/11.

92. *Criterion 7.5* (Mostly met)

a) Sec. 50 of TOCFR permits addition to the accounts frozen pursuant to UNSCRs 1718 or 1737 of interests or other earnings due on those accounts or payments due under contracts, agreements or obligations that arose prior to the date on which those accounts became subject to the provisions of this resolution. Interest, other earnings and payments continue to be subject to these provisions and are frozen.

b) Schedule 2 to the TOCFR, which sets out requirements for freezing orders for terrorism and proliferation-related purposes, includes provision for the issue of licences which could or would be used to authorise the use or release of funds where permitted by an exemption. However, the legislation is silent on conditions laid down in C 7.5 (b). However any licence relating to proliferation sanctions would have to be in accordance with the provisions of the relevant UN or EU sanctions legislation (for example, UNSCR 1737, as implemented in the IoM by means of applying EU Reg. 267/2012). The crediting of interest to frozen accounts, and other permitted payments into and from frozen accounts, would be allowed if authorised by the relevant legislation (e.g. para. 2 of Schedule 2 to TOCFR).

Weighting and Conclusion

93. The IoM meets c.7.1, 7.2 and mostly meets c.7.3, 7.4 and 7.5. **R.7 is rated largely compliant.**

Recommendation 8 – Non-profit organisations

94. In the 2009 Report, the IoM was rated largely compliant for the former SR VIII (para. 916 to 934). Two main shortcomings were identified: a review of NPO laws and regulations had not yet been complete; and the coverage of the legislation excluded NPOs that were not charities.

95. Since the last evaluation, the IoM has undertaken a review of the legislative framework (as described below under C 8.1(a)) and extended the coverage of the AML/CFT Code to SNPOs. SNPOs are defined in POCA 2008 and must be registered. The provisions of the Charities Registration Act 1989 (CRA 1989) and CR 2007 remain valid.

96. *Criterion 8.1* (Mostly met) - (a) - Within the context of the NRA, the adequacy of existing legislation related to NPOs was analysed from the perspective of potential FT threats and vulnerabilities. This analysis resulted in application of the AML/CFT Code and DBRO Act to NPOs. Nevertheless, the extension does not include all NPOs and applies only to those considered as being most vulnerable. They are referred to as SNPOs (Schedule 4 to POCA 2008 and Schedule 1, part 1 to DBRO Act).

97. (b) A detailed analysis of the NPO sector was conducted in April 2014. The process was led by the IOMFSA. Two other key institutions – the Central Registry and UK's National Crime Agency were also involved. With regard to the quantitative data on features and types of NPOs that are at risk of being misused for FT purposes, analyses were based mainly on information held about charities, as there was no information at that time on the non-charitable NPO sector. Such information will be analysed during the next assessment of the sector which is planned for 2016 and will take into account registered SNPOs.

98. (c) As mentioned under sub-criterion (b), reassessment of the sector will be conducted in April 2016. It will also take into consideration the new information about the non-charitable NPOs registered under the DBRO Act, which fall under the category of SNPOs.

99. *Criterion 8.2* (Met) - Two outreach sessions were conducted in October 2014 and October 2015. The first targeted the charitable sector and the second one included SNPOs.

100. *Criterion 8.3* (Met) - The IoM has included SNPOs within the scope of the AML/CFT Code to ensure their transparency and integrity.

101. *Criterion 8.4* (Mostly met) - At the time of 2009 Report, the only NPOs that had to fulfil the registration and monitoring requirements were charities (CRA 1989). Subsequently, legislation was amended and the registration obligation expands now to SNPOs. When deciding which NPOs

fall under this category, both size and activity are determinant key factors. According to Schedule 4 of POCA 2008, a SNPO must have: (i) an annual income of GBP 5 000 or more; and (ii) remitted, or is anticipated to remit, at least 30% of its income in any one financial year to one or more ultimate recipients in, or from, one or more higher risk jurisdictions. Such a risk based approach ensures that the regulated NPO sector covers: (i) a significant portion of the financial resources under the control of the sector; and (ii) a substantial share of the sector's international activities. Some of the requirements of c. 8.4 are not applicable equally for all regulated NPOs – charities and other SNPOs. For example, charities which are not SNPOs do not have to follow the "know your beneficiaries and associated NPOs" rule or maintain records for at least 5 years. Likewise, non-charitable SNPOs are not required to provide information to the Central registry on their management or administration.

Charities

102. (a) At the time of registration, charities must file information on name, purpose and objectives of their activities and on the identity of the persons who will own, control or direct their activities. This information is publicly available online through the Central Registry. Likewise, the Chief Registrar shall permit any person, who so requests, to have access to this information (Reg. 4 of the CRA 2007[74]). Information must be maintained by the charity under sec. 2 of the CRA 1989. The Act requires that any changes to information are notified to the Registrar within 1 month. Reg. 4 states that the Chief Registrar must permit any person to have access to that information. A detailed analysis on the maintained information under CRA 1989 can be found in para. 923 to 924 of the 2009 Report.

103. (b) As described by the 2009 Report (see para. 921), all charities are required to produce financial statements every calendar year (sec. 5 of the CRA 1989).

104. (c) The type of controls depends on the charity's turnover: internal control; external examination; statutory audit. Since 2011, the turnover threshold for an independent external examination or an audit was increased from £5,000 to £25,000 (up to £250,000). Consequently, a statutory audit will be required for charities with a turnover above £250,000 per annum. Controls are not specifically focused on elements of ML or TF, but they can ensure that all funds are fully accounted for and spent in a manner consistent with the organisation's purposes.

105. (d) Charities are required to register under CRA 1989 (sec. 2). Charities which fulfil the conditions to be considered Specific NPOs ((a) an annual income of £5,000 or more; and (b) remitted, or is anticipated to remit, at least 30% of its income in any one financial year to one or more ultimate recipients in or from one or more higher risk jurisdictions) must also be registered under DBRO Act (Part 2). Nevertheless, as described by 2009 Report in para. 916, there are some exemptions from the registration obligation which are provided by CRA 1989 (sec. 2(3)), CR 2007 and RCR 1999. However according to authorities these exemptions do not apply to the DBRO Act.

106. (e) and (f) These requirements do not apply for charities which are not SNPOs.

Specified NPOs

107. (a)-(c) Requirements under sub-criteria (a) to (c) on the level of maintained information are not applicable for non-charitable Specified NPOs.

108. (d) Specified NPOs are required to be registered under Part 2 of the DBRO Act. The registration obligation does not apply to all NPOs and targets only those who fulfil the conditions provided by POCA 2008, Schedule 4.

[74] This obligation could not be checked as Regulation 4 is not included in the version of CR 2007 provided by the authorities.

109. (e) SNPOs are obliged to identify their "customers" within the context of both a new or an existing business relationship (para. 17 and 18 of the AML/CFT Code). The concept of "customer" seems to cover beneficiaries and associated NPOs. It covers "the persons, or groups of persons, who receive benefit (either directly or indirectly) for charitable, religious, cultural, educational, political, social or fraternal purposes" (Part 1 of the AML/CFT Code). The obligation extends to any correspondent non-profit organisation receiving funds on behalf of a customer. In relation to an occasional transaction, the identification and verification of a donor's identity is required (para. 19). The identification procedure has to be based on reliable, independent sources and must include the information on the nature and intended purpose of the business relationship. Charities which are not SNPOs do not have such an obligation.

110. (f) Specified NPOs are obliged to maintain records on transactions for at least 5 years after the end of the business relationship (para. 33 of the AML/CFT Code). This information will be made available to competent authorities if required. In the case of an investigation or enquiry, all relevant records must be retained as required by the competent authority. It is not clear if SNPOs are also obliged to maintain for at least 5 years: (i) information on persons who own, control or direct their activities; and (ii) annual financial statements. Such an obligation is not provided by the AML/CFT Code. Record keeping obligations do not apply to other non-SNPOs charities.

111. *Criterion 8.5* (Met) - Only SNPOs are subject to periodic monitoring. The monitoring (oversight) includes: (i) annual declarations on compliance with the AML/CFT obligations; and (ii) on-site inspections and investigations (Part 3 of the DBRO Act). In light of information provided by the authorities all SNPOs will be subject to on-site visits within 3 years of the DBRO Act entering into force. The monitoring programme is a 6 yearly rolling programme, where entities might be visited every 2, 4 or 6 years, depending on the TF risk they pose. Other charities are not subject to periodic monitoring for AML/CFT purposes. Nevertheless, as described in the 2009 Report, the CRA 1989 provides for criminal penalties on trustees, directors, managers or similar officers, who breach statutory obligations (para. 926). SNPOs can be sanctioned for failing to comply with the AML/CFT Code (para. 41) and failing to provide information under the DBRO Act (sec. 20).

112. *Criterion 8.6* (Mostly Met) - (a) In addition to the statutory gateways described by the previous assessment report (para. 931), new gateway powers have been introduced under DBRO Act. Exemptions to prohibitions on disclosure are allowed for the purpose of enabling or assisting the Collector of Customs and Excise to discharge the Collector's functions (Schedule 2 of the DBRO Act).

113. (b) Under Reg. 4 of the CR 2007, the Chief Registrar is obliged to make available to any person information on the administration and management of any charity. Such data is also available to the authorities via the Central Registry. Legislation does not impose a similar requirement for non-charitable SNPOs. Thus, it is not clear if the authorities have access to such information in relation to SNPOs which are not charities nor what would be the source of such information.

114. (c) A disclosure can be made to the FIU under POCA 2008, for suspected ML, and under ATCA, for suspected TF. SNPOs which are considered to be at a higher risk of being abused for TF are part of the regulated sector and have the ability to file SARs to the FIU. Other NPOs may report their suspicions to the IoM Constabulary or the FIU.

115. *Criterion 8.7* (Met) - Formal requests for assistance are made through the AGC, which is the central authority (see para. 934 of the 2009 Report).

Weighting and Conclusion

116. The IoM meets c.8.2, 8.3, 8.5 and 8.7. It mostly meets c.8.1, 8.4 and 8.6. **R.8 is rated largely compliant**.

Recommendation 9 – Financial institution secrecy laws

117. In its 2009 Report, the IoM was rated largely compliant with former R.4 (paras. 574 to 578). It was noted that there was no explicit provision enabling FIs to exchange customer information with other institutions. To a large extent, this matter has been addressed by an amendment to POCA in 2009.

118. *Criterion 9.1.* (Met) - Although there is strict application by FIs of the common law duty of confidentiality in respect of customer information, it is overridden by various statutory provisions including: (i) POCA 2008 and the ATCA which provide statutory protection against any criminal or civil action for making a report to the FIU; (ii) POCA 2008, the Criminal Justice Acts 1990 and 1991 and the PPPA 1998 which enable competent authorities to access and share evidence domestically and internationally (sec. 21 of the Criminal Justice Act 1991 includes the primary power used to execute requests for MLA); (iii) sec. 34 of the FSA 2008 and Schedule 5 of the IA 2008 which allow the IOMFSA to exercise its powers for and on behalf of, and share information with, another regulatory authority (in the IoM or overseas); and (iv) schedule 2 of the DBRO Act which allows the IOMFSA to share information with a competent authority (in the IoM or overseas).

119. Sec. 147 of the POCA (2008) also overrides the duty of confidentiality and empowers FIs to exchange information where necessary for AML/CFT purposes and where this is required by R. 13, 16 or 17.

Weighting and Conclusion

120. **R.9 is rated compliant.**

Recommendation 10 – Customer due diligence

121. In the 2009 Report, the IoM was rated partially compliant with these requirements, and the Report identified five deficiencies (paras. 405 to 518). The deficiencies identified in the 2009 Report appear to have been remedied through the issuance of revised Codes and Rules (as indicated in MONEYVAL's 3rd Round progress report adopted in 2013). R.10 was subject to significant revisions in 2012, and the AML/CFT Code was amended in April 2015 to address some of the new requirements of R.10.

122. Not all of the activities or operations listed in the FATF's definition of "financial institution" are regulated or supervised[75]. The effect of the scope gap is thought to be minor.

123. *Criterion 10.1* (Met) - Para. 40 of the AML/CFT Code does not permit a FI to set up, or maintain, an anonymous account or an account in a name that it knows or has reasonable cause to suspect to be fictitious for any new or existing customer. This prohibition does not apply to three long-term insurance policies with an aggregate value of less than EUR 66 000 (as of December 2015) which were all issued prior to 1990 (when there were no CDD requirements) and which cannot be terminated under the terms of the contract. Reg. 15 of the IAMLR 2008 will require the application of ECDD measures to these three policies at the time that they are surrendered or payment is made. Given the number of accounts involved (and value) and measures in place to mitigate risk, this criterion is considered to be met.

124. *Criterion 10.2* (Partly met) - Para. 10 of the AML/CFT Code requires CDD procedures to be undertaken in line with c.10.2 (a) to (c). CDD procedures are also required under para. 11(3)(d) of the AML/CFT Code in any case where evidence of identity produced under para. 10(1) is not for any reason "satisfactory". Here, "evidence of identity" is defined broadly to include the identification and verification of identity, verification of legal status, information on the nature

[75] Schedule 4 of the POCA 2008 does not cover all elements of: (i) participation in securities issues and provision of financial services related to such issues; or (iii) investing, administering or managing funds or money on behalf of other persons.

and purpose of the relationship, and information on source of funds. The authorities have explained that the term "satisfactory" will cover the case where there is doubt about the veracity or adequacy of previously obtained customer identification data (c.10.2(e)).

125. There is no requirement in the AML/CFT Code to undertake CDD measures when there is suspicion of ML or TF (c.10.2(d)) though para. 15(2) requires a FI to consider whether to obtain enhanced CDD in the event of any suspicious activity and para. 15(3) rules out the use of simplified CDD and all but one CDD exemption in any case where a higher ML/TF risk is applied.

126. *Criterion 10.3* (Met) - Para. 10 and 12 of the AML/CFT Code require FIs to establish, maintain and operate procedures for: (a) the identification of the customer; (b) the verification of the identity of the customer using reliable, independent source documents (including information recorded in any form); and (c) the verification of the legal status of the customer using relevant information obtained from a reliable, independent source. Definitions provided under para. 3 of the AML/CFT Code cover permanent or occasional customers and customers that are natural persons, legal persons or legal arrangements.

127. *Criterion 10.4* (Partly Met) - Pursuant to paras. 13(3)(a) and 13(3)(b) of the AML/CFT Code, FIs are required to: (a) verify that any person purporting to act on behalf of a legal person or legal arrangement is so authorised; and (b) identify that person and take reasonable measures to verify the identity of that person (rather than identify and verify the identity of that person - in line with the standard) using reliable and independent source documents. However, there is no obligation in the AML/CFT Code to apply such measures to a person purporting to act on behalf of customer who is an individual.

128. Despite this, sec. 4.20 of the IGN (considered to be "other enforceable means") requires that, where an application for a business relationship has persons other than the applicant and beneficiaries who are able to exercise significant control over the assets (e.g. an investment advisor on a personalised bond), the insurer must establish procedures for verifying the identity of the that person. In addition, sec. 4.2 of the AML/CFT Handbook (guidance) also provides that, in circumstances where a customer appoints another person as an account signatory e.g. an expatriate appointing a member of his family, full CDD procedures should also be carried out on the new account signatory or attorney in accordance with para. 13 of the AML/CFT Code.

129. *Criterion 10.5* (Partly met) - Pursuant to para. 13(2) of the AML/CFT Code, FIs are required to: (i) identify the beneficial owner of a customer that is not a natural person and take reasonable measures to verify the identity of that beneficial owner, using relevant information obtained from a reliable, independent source; and (ii) determine whether the customer is acting on behalf of another person, and, if so, identify that other person and take reasonable measures to verify that other person's identity using information obtained from a reliable, independent source.

130. As explained under c.1.6, the AML/CFT Code exempts (in strictly controlled circumstances) certain FIs from the requirement to identify and verify the identity of: (i) certain customers (and their beneficial owners or controllers) under para. 20; and (ii) persons on whose behalf a customer is acting under para. 21. Whilst these exemptions are considered to be in line with examples provided in the IN to R.10, para. 20 may be applied to lawyers and accountants that are not members of professional self-regulatory bodies and which have only very recently registered under the DBRO Act, and para. 21 may be applied where a customer acting on behalf of a third party has been assessed as posing a higher risk of ML/TF. This has a cascading effect on c.10.5.

131. *Criterion 10.6* (Met) - Under paras. 10(3)(d) and 12(3)(d) of the AML/CFT Code, FIs are required to maintain and operate procedures for obtaining information on the nature and

intended purpose of the business relationship[76]. Para. 4(3) of the AML/CFT Code also requires procedures to enable a FI to manage and mitigate its ML/TF risks in line with its assessment of the risk for a particular customer. As part of on-going CDD, para. 11(3)(a) of the AML/CFT Code also requires FIs to examine the background and purpose of a business relationship once a business relationship has been formed.

132. *Criterion 10.7* (Met) - Paras. 9(1)(c)(i) and 9(1)(a) of the AML/CFT Code require FIs to perform on-going due diligence in line with c10.7. In scrutinising transactions, FIs must also ensure that they are consistent with its business risk assessment, customer risk assessment and technological developments risk assessment under paras. 6, 7, 8 of the AML/CFT Code. The extent and frequency of any such monitoring must be determined on the basis of materiality and risk of ML/TF: para. 9 (2) of the AML/CFT Code. Para. 11(3)(a), (c) and (d) of the AML/CFT Code are also relevant.

133. *Criterion 10.8* (Met) - There is a general requirement for FIs to gather information concerning the nature of a business relationship when applying CDD measures in respect of all customers (including legal persons and legal arrangements), as described under c.10.6. Also, para. 7(3)(b) of the AML/CFT Code requires FIs to understand the nature, scale, complexity and location of the customer's activities when dealing with the customer risk assessment. FIs are required to obtain information to understand the ownership and control structure of each customer that is a legal person or legal arrangement: para. 13(3)(g) of the AML/CFT Code.

134. *Criterion 10.9* (Met) - Paras. 10, 12, 13 and 23 of the AML/CFT Code require FIs to identify and verify the identity of legal persons and legal arrangements in line with c.10.9. Whilst the AML/CFT Code does not directly require identification of a legal person or legal arrangement to include collection of the address of the registered office (or, if different, principal place of business), sec. 4.5.2 to 3, 4.6.2 to 3, and 4.8 to 9 of the AML/CFT Handbook and sec. 4.3 to 4.15 of the IGN provide comprehensive guidance on how to identify a legal person or legal arrangement, including information on registered address (or business address if different).

135. *Criterion 10.10* (Met) - Inter alia, para. 13 of the AML/CFT Code specifies that FIs are required: (i) to identify who is the beneficial owner of the customer where the customer is not a natural person; and (ii) take reasonable measures to verify the identity of any beneficial owner of the customer. Inter alia, "beneficial owner" is defined in para. 3 of the AML/CFT Code as the natural person who ultimately owns or controls the customer and includes, but is not restricted to: (a) in the case of a legal person other than a company whose securities are listed on a recognised stock exchange, a natural person who ultimately owns or controls (through direct or indirect ownership or control) 25% or more of the shares or voting rights in a legal person; and (b) a natural person who otherwise exercises ultimate effective control over management of the legal person. These requirements appear to be broadly in line with the requirements of c.10.10, and to cover cases where any person identified is not an individual, where it would be necessary to look through to the natural person(s) who ultimately owns or exercises control over the legal person.

136. As regards companies, para. (a) would cover individuals that have a controlling ownership interest, while para. (b) would cover individuals exercising control through other means or through the company management.

137. In the case of a foundation, para. 13(3)(d) to (f) of the AML/CFT Code requires the following to be identified: (i) council members; (ii) known beneficiaries; (iii) founder and any other "dedicator"; (iv) other natural persons having a power to direct the customer's activities (which may include a guardian); and (v) persons who may impose binding obligations on the customer. Guidance in the Handbook explains that it is also necessary to obtain information on other

[76] Inter alia, sec. 4.13 of the AML/CFT Handbook explains that the following information should be obtained: expected type, volume and value of activity; and expected geographical sphere of the activity; and details of any existing relationships with the product/service provider.

persons with a "sufficient interest", including a person who, in the view of the High Court, can reasonably claim to speak on behalf of an object or purpose of the foundation.

138. *Criterion 10.11* (Mostly met) - Paras. 13(3)(c), (e) and (f)) and 13(5) of the AML/CFT Code apply to legal arrangements and require identification of: (i) the trustee(s) or any other controlling party; (ii) known beneficiaries (but not also classes of beneficiaries)[77]; (iii) the settlor "or other person by whom the legal arrangement is made or on whose instructions the legal arrangement is formed"; (iv) other natural persons having power to direct the customer's activities (which may include the protector); (v) persons who may impose binding obligations on the customer; and (vi) those persons who are to receive benefit from the trust. Whilst the authorities have explained that it will be necessary to obtain information on classes of beneficiaries (and to have capacity to be able to establish the identity of any beneficiary in the future) in order to assess the risk of a business relationship or occasional transaction in respect of a trust (para. 7 of the AML/CFT Code), there is no explicit requirement to obtain and hold this information. In contrast, sec. 4.5 of the IGN states that, where an applicant is a trustee, the insurer must: (i) be satisfied that it has been provided with details of beneficiaries defined only by class; (ii) satisfy itself that the class does exist; and (iii) satisfy itself that it has sufficient information to identify members of such a class.

139. Paras. 13(3)(c), (e) and (f) and 13(5) of the AML/CFT Code and guidance in the AML/CFT Handbook do not explain the additional measures that will be needed where the customer (trustee) is acting under para. 13(2)(c) on behalf of another person who is not an individual.

140. Para. 13 of the AML/CFT Code is written broadly and refers to legal arrangements rather than specifically to trusts. The same provisions would apply then to any other arrangement that has a similar legal effect to a trust.

141. *Criterion 10.12* (Partly met) - Para. 13(4) of the AML/CFT Code requires an insurer to: (i) identify the beneficiaries of a life assurance policy; and (ii) verify the identity of each such beneficiary using relevant information obtained from a reliable, independent source - immediately prior to making any payment or loan. Art. 13(4) of the AML/CFT Code does not also cover other investment related insurance policies. Nor does this paragraph require a FI to obtain sufficient information to satisfy itself that it will be able to establish the identity of the beneficiary of a life assurance policy that is not specifically named but instead designated by characteristics, class or other means at the time of pay-out. However, in a case where a trust is the beneficiary of a life insurance policy, guidance provided in sec. 4.5 of the IGN states that the trustee will disclose any class of beneficiaries to the FI, and FI take whatever steps are necessary to be satisfied that the class exists.

142. *Criterion 10.13* (Partly met) - The AML/CFT Code does not explicitly require information about the beneficiary of a life assurance policy to be taken into account as a relevant risk factor when considering whether there is a need to apply enhanced CDD measures at the start of, or during, a business relationship. However, para. 7 of the AML/CFT Code does require a FI to have regard to the persons to whom, and manner in which, products and services are provided, when assessing customer risk, and the authorities have explained that they would expect insurers to consider all parties named in an application, including nominated beneficiaries. Whereas para. 15 of the AML/CFT Code requires a FI to apply enhanced CDD measures where a customer relationship (including with a legal person or legal arrangement) poses a higher risk, such measures may not include reasonable measures to identify and verify the identity of the beneficial owner of that

[77] In line with sec. 5 of the sector specific guidance for TCSPs in the AML/CFT Handbook, where a potential beneficiary (who may be part of a class) is merely an object of a power and at best only has a hope of benefiting from the trust at the discretion of the trustees at some time in the future, the TCSP would be also be expected to know the name of this individual.

beneficiary at the time of pay out, in a case where the beneficiary is a legal person or legal arrangement[78].

143. *Criterion 10.14* (Met) - FIs are required to undertake procedures for verifying the identity of the customer and beneficial owner before establishing a business relationship or conducting transactions for occasional customers pursuant to para. 10 (2), 12 (2), 13 (1), 23 (3) of the AML/CFT Code. In exceptional circumstances, such procedures may allow verification of the identity of the customer to be undertaken following the establishment of the business relationship, if the conditions under c.10.14 (a)-(c) are met: para. 10 (4) of the AML/CFT Code.

144. *Criterion 10.15* (Met) - The AML/CFT Code sets out risk management requirements for use of this timing concession under para. 10. In particular, para. 10(4)(e) requires senior management to approve the establishment of the business relationship and any subsequent activity until the customer's identity has been verified and para. 10(4)(f) requires a FI to ensure that the amount, type and number of transactions is appropriately limited and monitored. If a higher risk of ML/TF is assessed then this timing concession does not apply.

145. *Criterion 10.16* (Met) - Para. 11(2) of the AML/CFT Code requires FIs to apply CDD measures to existing customers as soon as "reasonably practicable", taking account of the overriding requirement in para. 4(4) to: (i) apply CDD measures on the basis of materiality and risk; and (ii) have particular regard for whether a customer poses a higher risk of ML/TF. Para. 11(3)(b) of the AML/CFT Code applies when no evidence of identity has been produced and 11(3)(c) and (d) to a case where evidence was previously collected but is no longer satisfactory. Sec. 4.4.1 of the AML/CFT Handbook explains that, generally, identification measures should be applied within 3 months of the legislation coming into effect. However, there may be flexibility on this timescale, such as where a FI has a particularly large customer base and 3 months is therefore impractical. Where such a decision is made on the grounds of impracticality, the rationale behind this should be documented and the IOMFSA should be informed of the FI's proposed timetable to remediate this.

146. CDD requirements for existing customers are also set out in Reg. 18(1)-(3) of the IAMLR and sec. 5.1-5.2 of the IGN.

147. *Criterion 10.17* (Met) - FIs are required to perform enhanced due diligence where the ML/TF risks are higher pursuant to para. 15 of the AML/CFT Code which specifically deals with ECDD. Para. 15 has a general requirement for FIs to perform ECDD where a customer poses a higher risk of ML/TF as assessed by the customer risk assessment (required under para. 7 of the AML/CFT Code) as well as in the event of any unusual activity, and in addition to that, lists some specific matters that pose (e.g. connection with a customer resident or located in a country with strategic ML/TF deficiencies) or may pose a higher risk of ML/TF (e.g. a company that has nominee shareholders or shares in bearer form, PEPs, etc.).

148. Para. 15 must be read alongside para. 4(3) of the AML/CFT Code which includes an overriding requirement that enhanced CDD applied must be commensurate with risks.

149. *Criterion 10.18* (Met) - The AML/CFT Handbook anticipates that simplified CDD measures will be applied under the AML/CFT Code only in exceptional circumstances - where a FI considers a particular customer as presenting a lower risk of ML/TF than those customers assessed as standard risk. Where a customer presents a lower risk of ML/TF, sec. 3.3.1 of the AML/CFT Handbook explains that methods of verification of identification may be "less robust".

150. The issue of application of simplified CDD measures is also dealt with in Part 6 of the AML/CFT Code (along with exemptions from the application of particular CDD measures). In a case where

[78] Whilst para. 13(4)(b) of the *AML/CFT Code* requires the identity of every beneficiary of a life policy (including a beneficiary who is a legal person or legal arrangement) to be verified immediately prior to payment, this requirement does not also extend to the beneficial owner of that beneficiary.

an annual insurance premium is less than EUR 1 000, or single premium is less than EUR 2 500, a life assurance company can defer the application of CDD measures until such time as a claim is made or policy cancelled (para. 24(1) to (6) of the AML/CFT Code). CDD measures may also be deferred in the case of an insurance contract that has no surrender or maturity value until such time as a settlement over EUR 2 500 is made (para. 24). However, simplified measures may not be applied if any suspicious activity has been identified or where the customer has been assessed as posing a higher risk of ML/TF.

151. *Criterion 10.19* (Mostly met) - Where satisfactory evidence of identity is not obtained or produced under paras. 10, 12 and 23 of the AML/CFT Code, procedures that are established, maintained and operated must require a potential business relationship to "proceed no further" or occasional transaction not to be carried out. Where satisfactory evidence of identity is not obtained or produced under paras. 11 and 23, procedures that are established, maintained and operated must require: (i) an existing business relationship to proceed no further; and (ii) consideration to be given to terminating the relationship. The effect of these provisions will be to freeze a business relationship (even in a case where a decision is taken not to terminate it). Where enhanced CDD cannot be obtained or produced under para. 15 of the AML/CFT Code, then the same provisions apply.

152. Paras. 26 to 28 of the AML/CFT Code also requires procedures in such cases to require an internal disclosure to be made to the MLRO when there is knowledge or suspicion that another person is engaged in ML/TF activity. The MLRO must assess the information contained within the internal disclosure to determine whether there are reasonable grounds for knowing or suspecting that the activity is related to ML/TF and consider making an external disclosure to the FIU.

153. *Criterion 10.20* (Partly met) - There is no provision that allows FIs not to perform CDD under paras. 10 to 12 of the AML/CFT Code if this would result in the customer being tipped-off. However, where a FI identifies any suspicious activity, it is required only to consider obtaining enhanced CDD under para. 15(2).

Weighting and Conclusion

154. The IoM meets c.10.1, 10.3, 10.6 to 10.10, and 10.14 to 10.18, and mostly meets c.10.11 and 10.19. It partly meets c.10.2, 10.4, 10.5, 10.12, 10.13 and 10.20. **R.10 is rated largely compliant**.

Recommendation 11 – Record-keeping

155. In the 2009 Report, the IoM was rated as compliant with these requirements. However, the applicable legislation has changed, so a new analysis has been undertaken.

156. *Criterion 11.1.* (Met) - Under paras. 32(b) and 33(1)(a) of the AML/CFT Code, FIs must keep all necessary records on transactions, both domestic and international, for at least five years following completion of the transaction. Additional record-keeping requirements are also placed on entities licensed under sec. 7 of the FSA 2008 (through the FSRB).

157. *Criterion 11.2.* (Mostly met) - Under paras. 32 (a) and 33(1)(b) of the AML/CFT Code, FIs are required to keep all records obtained through CDD measures for at least five years following the termination of the business relationship or after the date of the occasional transaction. The authorities consider that such records will include business correspondence, analysis, account files etc. However, account files, business correspondence, and results of any analysis undertaken are separately addressed under paras. 32(b) and 33(1)(a) of the AML/CFT Code which states that they must be kept for at least five years following completion of a transaction. This differs to the standard which requires accounts files, business correspondence and analysis to be kept for at least five years following termination of a business relationship or after the date of an occasional transaction. Accordingly, material that is held on accounts files and in business

correspondence that has not been collected through CDD measures may be destroyed ahead of the termination of a business relationship.

158. *Criterion 11.3.* (Met) - Para. 32 (c) of the AML/CFT Code requires transaction records to be sufficient to permit the reconstruction of individual transactions:

159. *Criterion 11.4.* (Met) - Para. 34 of the AML/CFT Code requires hard copy records to be capable of retrieval without undue delay if kept within the IoM, and available within no more than 7 working days if they are kept outside the IoM. If records are not in hard copy, the FI must ensure they are readily accessible in, or from, the IoM and are able to be retrieved without undue delay.

Weighting and Conclusion

160. The IoM meets c.11.1, 11.3 and 11.4 and mostly meets c.11.2. **R.11 is rated largely compliant**.

Recommendation 12 – Politically exposed persons

161. In its 2009 Report, the IoM was rated compliant with these requirements. However, since then, the FATF Standards have changed, and the IoM has further amended its legislation to implement the new requirements.

162. *Criterion 12.1.* (Met) - In relation to foreign PEPs, FIs are required to apply the four additional measures set out in c.12.1: paras. 4, 10(3)(e) and 14 of the AML/CFT Code. The term PEP is defined in detail in para. 3 of the AML/CFT Code, which closely follows the FATF definition.

163. *Criterion 12.2.* (Met) - In relation to domestic PEPs and persons who have been entrusted with a prominent function by an international organisation, FIs are required to apply the additional measures set out in c.12.2: paras. 4, 10(3)(e) and 14 of the AML/CFT Code.

164. *Criterion 12.3.* (Met) - The definition of a PEP in the AML/CFT Code includes a comprehensive list of family members and close associates of persons entrusted with a prominent public function. Accordingly, c.12.1 and c.12.2 apply also to family members and close associates.

165. *Criterion 12.4* (Partly met) - FIs in the IoM (including life insurers) are also required under para. 14(1)(c) of the AML/CFT Code to establish, maintain and operate procedures and controls for the purpose of determining whether any "known beneficiary" is a PEP, but not also to determine whether the beneficial owner of such a beneficiary is a PEP. In addition, para. 13(4) of the AML/CFT Code requires an insurer to identify the beneficiaries of a life assurance policy and, immediately prior to the making of any payment or loan, verify the identity of each such beneficiary. However, where necessary, these requirements do not also extend to the beneficial owner of such a beneficiary. Also, para. 13(5) of the AML/CFT Code states that a FI must not make a payment or loan to the beneficial owner of a legal person or beneficiary of a legal arrangement that is a customer until it has identified the recipient and, on the basis of materiality and risk, verified the identity of the recipient. This will be relevant where the beneficial owner of such a legal person or beneficiary of such a legal arrangement is also the beneficiary of a life policy held by such a person or arrangement.

166. In any case where a beneficiary of a life insurance policy is a foreign PEP or domestic PEP presenting a higher risk, FIs are required under para. 14(2) to (4) to: (i) have senior management approval; (ii) establish their source of wealth; and (iii) perform on-going and effective enhanced monitoring of the business relationship (which will identify cases where consideration must be given to making a STR under para. 27 of the AML/CFT Code). Additional requirements in relation to the manner in which relevant insurance businesses must deal with PEP relationships are provided in the IAMLR 2008 (Reg. 20) and IGN.

Weighting and Conclusion

167. The IoM meets c.12.1, 12.2 and 12.3 and partly meets c.12.4. Given the significance of the IoM's life assurance sector and gaps in applying measures to the beneficial owners of policy beneficiaries, **R.12 is rated largely compliant**.

Recommendation 13 – Correspondent banking

168. In its 2009 Report, the IoM was rated compliant with these requirements. Since then, the IoM has further amended its legislation and relatively minor changes were made to R.13, with c.13.3 being the only substantial addition.

169. *Criterion 13.1.* (Met) - FIs are required to apply the measures set out under c.13.1 in respect of cross-border correspondent relationships with respondent and correspondent institutions from third countries: para. 39(3)(a) to (e) of the AML/CFT Code.

170. *Criterion 13.2*. (Met) - Pursuant to para. 39(4)(a) and (b) of the AML/CFT Code, FIs are required to ascertain that the respondent institution has conducted due diligence on customers having direct access to the accounts of the respondent and is in a position to provide, upon request, relevant evidence of identity on these customers.

171. *Criterion 13.3.* (Met) - FIs are prohibited from entering into or continuing correspondent relations with shell banks, and must take appropriate measures to ensure their respondents do not permit accounts to be used by shell banks: paras. 38 and 39(2) of the AML/CFT Code. The definition of "shell bank" in para. 3 of the AML/CFT Code is consistent with the FATF definition.

Weighting and Conclusion

172. The IoM meets all three criteria. **R.13 is rated compliant**.

Recommendation 14 – Money or value transfer services

173. In its 2009 Report the IoM was rated largely compliant with these requirements (paras. 770-780). The deficiency identified related to the absence of active supervision of MVTS providers for AML/CFT purposes, which had not yet commenced at the time of the assessment.

174. *Criterion 14.1.* (Met) - Natural or legal persons that provided MVTS are required to hold a class 8 licence (RAO 2011) under sec. 4(1) of the FSA 2008 where they provide such services: (i) directly; or (ii) as agent. Accordingly, where a MVTS operates through an agent, the agent (e.g. the IoM Post Office) must be registered but not also the principal (e.g. MoneyGram). The IOMFSA's website provides a register of current and former licence holders.

175. *Criterion 14.2.* (Met) - In order to identify natural or legal persons that carry out MVTS without a licence, the IOMFSA regularly monitors the local press and considers the activities of client businesses as a part of its on-going supervisory visits of FIs. Any business undertaking regulated activity under the *FSA 2008* without the requisite licence is liable on summary conviction (lower court) to a fine not exceeding £5,000 and/or imprisonment not exceeding 2 years, or otherwise (higher court) to an unlimited fine and/or imprisonment not exceeding 2 years. In addition to this sanction, the IOMFSA could also liquidate a company undertaking unlicensed business (public interest grounds) under the Companies Act 1931. Regulatory sanctions may also be taken against unauthorised business – as explained under R.35.

176. *Criterion 14.3.* (Met) - MVTS providers are subject to the IOMFSA's on-going supervisory monitoring of compliance with AML/CFT legislation, including off-site collection of information. In line with registration requirements, agents of MVTS operators (e.g. the IoM Post Office) are subject to monitoring for AML/CFT purposes (rather than the principal, e.g. MoneyGram, whose systems are used).

177. *Criterion 14.4.* (Met) - See c.14.1. The IOMFSA keeps an on-line register of these agents.

178. *Criterion 14.5.* (Partly met) - According to Rule 6.71 of the FSRB, an authorised payment service provider (principal) who wishes to provide services through an agent must assess the agent and be satisfied that it holds the necessary regulatory permissions and also demonstrate competence in relation to this business. Under the same rule, the agent must also enter into terms of business with the principal. The principal must also notify the Authority, not less than 20 business days in advance, of the appointment of any new agencies or changes in existing agencies. However, there is no clear obligation for a payment service provider that operates through agents in the IoM to include agents in its AML/CFT programmes or to monitor them for compliance with these programmes, though sec. 7 of the FSA 2008 states that the principal's risk management policies should consider all material risks.

Weighting and Conclusion

179. The IoM meets c.14.1 to 14.4 and partly meets c.14.5. **R.14 is rated largely compliant**.

Recommendation 15 – New technologies

180. In its 2009 Report the IoM was rated largely compliant with previous misuse of technological development requirements (see paras. 540 to 549). Some deficiencies were identified, including the lack of evidence of special attention to specific ML/TF risks of new technologies, including in relation to e-money and e-commerce, and no evidence of testing by the authorities of implementation by FIs of appropriate measures. Since then the FATF standards relating to the risks posed by new technologies have changed substantially.

181. *Criterion 15.1.* (Met) - Pursuant to paras. 6 and 8 of the AML/CFT Code, FIs are required to carry out: (i) a business risk assessment; and (ii) an assessment that estimates the risk of ML/TF posed by any technological developments. These cover the risks set out under c.15.1.

182. The authorities identify and assess these ML/TF risks as part of the NRA. In addition, the IOMFSA considers these risks when it is notified by a FI of any material changes to activities, services or products under Rule 8.10 of the FSRB.

183. *Criterion 15.2.* (Met) - Pursuant to para. 8 (2)(a) and (b) of the AML/CFT Code, FIs are required to undertake a risk assessment prior to the launch/implementation of new products, business practices and delivery methods (including delivery systems). A risk assessment must also be undertaken prior to the use of developing technologies for both new and pre-existing products. Technological developments must also be considered as part of the business risk assessment required under para. 6 of the AML/CFT Code. In support of these provisions, para. 4(3) and para. 9 of the AML/CFT Code also require FIs to take appropriate measures to manage and mitigate the risks (as part of normal CDD measures).

Weighting and Conclusion

184. The IoM meets both criteria. R.15 is **rated compliant**.

Recommendation 16 – Wire transfers

185. In the 2009 Report the IoM was rated largely compliant with these payments requirements (see paras. 599 to 616). Two deficiencies were identified: the need to improve the application of the risk-based approach when dealing with wire transfers that lack full originator information; and the need to strengthen the monitoring of compliance with wire transfer requirements by the supervisory authorities. Since then, significant changes have been made to requirements in this area during the revision of the FATF standards.

186. The IoM implements (with appropriate modifications) the requirements on wire transfers set out in Reg. (EC) No. 1781/2006 (EU Reg. on Wire Transfers), by means of orders made by the Council of Ministers (which constitutes secondary legislation in the IoM). In the previous round of assessments, the EU Reg. on Wire Transfers was determined to be compliant with former SR.VII. However, the revision of the Recommendations has introduced certain new requirements,

in particular requirements regarding information on the beneficiary of a wire transfer, which have not yet been implemented across the EU (and, as a result, the IoM). With respect to the elements carried forward from former SRVII, the IoM is deemed to be compliant.

187. Updated Reg. (EU) 2015/847 will, in due course, repeal and replace the EU Reg. on Wire Transfers to fully implement R.16, and it is expected that updated legislation (which is being prepared) will come into effect in the IoM at the same time. The authorities have explained that it is not possible to take action ahead of the EU, as a result of a derogation in Art. 17 of the EU Reg. on Wire Transfers under which it is bound to apply the same rules as those established in the EU[79]. It should be noted that, in addition to having to comply with the EU Reg. on Wire Transfers, any entity that undertakes payment services in the IoM will also be subject to the requirements of the AML/CFT Code by virtue of being included in Schedule 4 to the POCA 2008 as a "relevant business".

188. *Criterion 16.1.* (Partly met) - FIs are required to ensure that all cross-border wire transfers of EUR 1 000 or more are accompanied by required and accurate originator information: EU Reg. on Wire Transfers – Art. 4 and 5. However, there is no requirement to ensure that such transfers are also accompanied by the required beneficiary information.

189. *Criterion 16.2.* (Partly met) - The requirements of the EU Reg. on Wire Transfers regarding batch files are consistent with c.16.2 regarding originator information: Art. 7.2. The originator information would also have to be known to the payment service provider under Part 4 of the AML/CFT Code. However, there is no requirement to include beneficiary information in the batch file.

190. *Criterion 16.3.* (Partly met) - Art. 3 of the EU Reg. on Wire Transfers sets the scope of the Reg. and includes some de minimis thresholds (applying to transfer of funds using electronic money or mobile phone or other digital advice). In such cases, Art. 5 no longer applies and so wire transfers need not be accompanied by complete information held on the payer. Under the EU Reg. on Wire Transfers, there is no requirement to ensure that such transfers are also accompanied by the required beneficiary information.

191. *Criterion 16.4.* (Partly met) - The EU Reg. on Wire Transfers requires collection (but not verification) of payer information in case of transactions less than EUR 1 000. As explained under c.10.2, there is no requirement in the AML/CFT Code to verify identity in a case where there is suspicion of ML or TF.

192. *Criterion 16.5. & 16.6.* (Met) - In relation to domestic wire transfers, Art. 6 of the EU Reg. on Wire Transfers provides that, where the payment service provider of the payer and the payment service provider of the payee are in the UK payment area (the UK and Crown Dependencies), transfers of funds shall be required to be accompanied only by the account number of the payer or a unique identifier allowing the transaction to be traced back to the payer. As per para. 2 of Art. 6 of the EU Reg. on Wire Transfers, if requested by the payment service provider of the payee the payment service provider of the payer shall make required and accurate information available within three working days of the request. Law enforcement authorities would also be able to compel immediate production of the information referred to above, pursuant to relevant provisions of the PPPA 1989, Part 4 of POCA 2008, Schedule 6 of ATCA and para. 1 of the Schedule to the Enforcement Regulations.

193. *Criterion 16.7.* (Met) - The ordering FI is required to retain complete information on the originator for five years: Reg. 5.5 of the EU Reg. on Wire Transfers. In addition, all FIs (including all entities executing wire transfers) are required to retain all records (including beneficiary information, where it exists) for a period of 5 years: paras. 32 and 33 of the AML/CFT Code.

[79] It is intended that the IoM's legislation will be submitted to the UK for transmission to the European Commission by the end of 2016.

194. *Criterion 16.8.* (Partly met) - Whereas it is an offence to fail to comply with the EU Reg. on Wire Transfers or applicable requirements in the AML/CFT Code, the execution of wire transfers that do not comply with requirements specified under c.16.1 to c.16.7 is not prohibited. The lack of requirements relating to beneficiary information also indirectly affects this criterion.

195. *Criterion 16.9.* (Mostly met) - Intermediary FIs are required to ensure that all originator information received and accompanying a wire transfer is kept with the transfer: Reg. 12 of the EU Reg. on Wire Transfers. However, there is no requirement to ensure that any accompanying beneficiary information is also retained with it.

196. *Criterion 16.10.* (Mostly met) - If the intermediary FI utilises a payment system with technical limitations, it must make all information on the originator available to the beneficiary FI upon request, within three working days, and must keep records of all information received for five years: Reg. 13 of the EU Reg. on Wire Transfers. The lack of requirements relating to beneficiary information also indirectly affects this criterion.

197. *Criterion 16.11.* (Partly met) - There is no requirement for intermediary institutions to take reasonable measures to identify cross-border wire transfers that lack originator or required beneficiary information. However, guidance published in sec. 11 of the AML/CFT Handbook states that intermediary institutions should have effective procedures for checking incoming wire transfers.

198. *Criterion 16.12.* (Not met) - There is no requirement for intermediary institutions to have risk-based policies and procedures for determining when to execute, reject, or suspend a wire transfer lacking originator or beneficiary information, and when to take the appropriate action.

199. *Criterion 16.13.* (Partly met) - Beneficiary FIs are required to identify whether the fields containing required information on the originator have been completed, and to have effective procedures to identify whether the required originator information is missing: Reg. 8 of the EU Reg. on Wire Transfers; and Part 4 of the AML/CFT Code. However, there are no obligations for missing beneficiary information.

200. *Criterion 16.14.* (Met) - A beneficiary FI is required to have procedures that require the identity of a customer who is the beneficiary of a cross-border transfer of EUR 1 000 or more to be verified: Part 4 of the AML/CFT Code. The record keeping requirements relating to CDD requirements would also apply: paras. 32, 33 of the AML/CFT Code.

201. *Criterion 16.15.* (Partly met) - If the required originator information is missing or incomplete, beneficiary FIs are required to either reject the transfer or ask for complete information, and take appropriate follow-up action in cases where this is repeated: Reg. 9 of the EU Reg. on Wire Transfers. However, there are no obligations relating to cases where the necessary beneficiary information is missing.

202. *Criterion 16.16.* (Met) - MVTS providers are subject to both the EU Reg. on Wire Transfers and AML/CFT Code.

203. *Criterion 16.17.* (Mostly met) - The relevant reporting requirements in POCA 2008 and ATCA require MVTS providers to make an STR to the FIU in relation to any suspicious wire transfer. Where the MVTS provider controls both the ordering and beneficiary side of a wire transfer, there is no requirement to also file a STR where another country is affected by the suspicious wire transfer. However, the FIU would disseminate the necessary information to its counterparts in affected jurisdictions.

204. *Criterion 16.18.* (Met) - FIs processing wire transfers are subject to the requirements of the EU regulations and domestic measures which give effect to UN resolutions 1267, 1373, and successor resolutions.

Weighting and Conclusion

205. The IoM meets c.16.5, 16.6, 16.7, 16.14, 16.16 and 16.18, and mostly meets c.16.9, 16.10 and 16.17. It partly meets c.16.1 to 16.4, 16.8, 16.11, 16.13, and 16.15, and does not meet c.16.12. **R.16 is rated partially compliant**.

Recommendation 17 – Reliance on third parties

206. The IoM was rated largely compliant in the 2009 MER (see paras. 550 to 573). The 2009 MER noted: (i) that not all permitted categories of introducer were subject to full AML/CFT requirements; and (ii) inconsistent application of CDD requirements by FIs, including in the case of insurers. This Recommendation is particularly important for the IoM, where a significant part of financial activities is conducted on a non-face-to-face basis and where introducers represent an important source of new and continuing business for FIs.

207. *Criterion 17.1* (Mostly met) - Para. 23 of the AML/CFT Code deals with eligible introducers. This allows a FI to place reliance on an introducer only to: (i) have verified the customer's identity (and also verified the identity of the beneficial owner of the customer); and (ii) hold on to that evidence of identity until it is called for - provided certain criteria are met. Accordingly, the AML/CFT Code does not permit reliance to be placed on an eligible introducer to perform all elements of (a) to (c) of the CDD measures set out in R.10.

208. An "eligible introducer" may be a: (i) "trusted person" – a third party that is regulated and supervised, or monitored, and which has measures in place for compliance with CDD and record-keeping requirements in line with R.10 and R.11 (but not a nominee company); or (ii) person in the same group as the relying FI - which not be regulated, supervised or monitored.

209. Other conditions must be met before reliance may be placed on an eligible introducer. In particular, there must also be a written agreement between the relying FI and the introducer to formalise their respective obligations, and this agreement must require the introducer to provide copies of identity documents immediately, when requested. Compliance with this agreement must be tested in order to ensure that relevant documents will be made available upon request and without delay. The ultimate responsibility for CDD measures remains with the FI relying on the third party.

210. *Criterion 17.2* (Met) - When determining in which countries the third party that meets the conditions can be based, the DHA takes into account information available on the level of country risk and publishes "List C" specifying jurisdictions which are considered to operate laws equivalent to those of the IoM.

211. *Criterion 17.3* (Met) - There are no specific provisions that change the way in which an FI must meet its requirements when the third party is part of the same financial group.

Weighting and Conclusion

212. The IoM meets c.17.2 and 17.3 and mostly meets c.17.1. **R.17 is rated largely compliant**.

Recommendation 18 – Internal controls and foreign branches and subsidiaries

213. In the 2009 Report, the IoM was rated largely compliant with R.15 and compliant with R.22. It was noted that the legislation did not require FIs to maintain an adequately resourced and independent audit function to test compliance with AML/CFT procedures (having regard to the size and nature of the business). Since then the obligations of R.18 have changed.

214. *Criterion 18.1* (Mostly met) - Except as highlighted below, the requirements set out under this criterion are broadly covered by paras. 4, 29, 30, and 31 of the AML/CFT Code. These include procedures to deal with new staff appointments and staff training.

215. There is no specific requirement in the AML/CFT Code to appoint a compliance officer at management level. However, FIs licenced under the FSA 2008 and subject to the FSRB are required to appoint a compliance officer who has, amongst other things, direct access to

responsible officers and appropriate status within the FI (the effect of which will be to require that officer to be appointed at management level). In the case of life assurance companies, para. 13 of the Corporate Governance Code of Practice for Regulated Insurance Entities (CGC) requires an on-going and effective compliance function that is adequate and appropriate to the nature, scale and complexity of the regulated entity, its activities and the risk to which it is exposed. This includes the compliance function having adequate and appropriate expertise, resources and authority to carry out its activities effectively. Whilst there is no requirement for a compliance officer per se to be appointed, both the IAMLR 2008 and IGN make reference to there being such a post-holder (who will sit in the life assurance company's compliance function). Whilst there is no requirement in the RBSA 2000 or DBRO Act for compliance management arrangements to be in place, the vast majority of FIs are subject to a requirement to have a compliance function or officer with appropriate status or authority.

216. There is no specific requirement in the AML/CFT Code in relation to having an independent audit function. However, the following rules in the FSRB are relevant: (i) Rule 8.31A - which requires banks to have an internal audit function or to be subject to a group internal audit function (though there is no requirement for such functions to consider AML/CFT matters); and (ii) Rule 8.6 – which requires entities licensed under the FSA 2008 to establish and maintain comprehensive policies appropriate to the nature and scale of their business. Policies must include appropriate independent internal audit and compliance procedures to test compliance with regulatory requirements (including the AML/CFT Code). In relation to insurers, sec. 12 of the CGC sets out the requirements for all insurance entities to have an ongoing and effective internal audit function that is adequate and appropriate to the nature, scale and complexity of the insurer, its activities and the risks to which it is exposed and which, inter alia, has appropriate independence from the operational activities it audits. Overall, the vast majority of FIs are therefore subject to a requirement to have an independent audit function.

217. *Criterion 18.2* (Not met) - Notwithstanding requirements that are placed on branches and subsidiaries to takes measures consistent with the AML/CFT Code (see below), there is no specific requirement in the AML/CFT Code for financial groups to have group-wide programmes against ML/TF. Despite this, the AML/CFT Handbook recommends the establishment of a group-wide AML/CFT policy to protect both a FI's global, and local, reputation.

218. *Criterion 18.3* (Mostly met) - A FI must ensure that any branch or subsidiary in a jurisdiction outside the IoM takes measures consistent with the AML/CFT Code and guidance issued by a competent authority: para. 37 of the AML/CFT Code. If the required measures in the other jurisdiction differ from the AML/CFT Code, the FI must ensure that any branch or subsidiary located in that other jurisdiction applies the higher standard. If a branch or subsidiary is unable to take consistent measures or apply the higher standard because the laws of the other jurisdiction prohibit it, the FI must inform the relevant IoM competent authority. However, such a FI is not required to apply appropriate additional measures to mitigate the ML/TF risks, though the IOMFSA has powers to require these measures to be applied.

Weighting and Conclusion

219. The IoM mostly meets c.18.1 and 18.3. It does not meet c.18.2. **R.18 is rated largely compliant**.

Recommendation 19 – Higher-risk countries

220. In the 2009 Report, the IoM was rated largely compliant given the fact that the process in place to ensure that FIs are advised of concerns about weaknesses in the AML/CFT systems of other countries had not been formalized. Since then the obligations of R.19 have changed significantly.

221. *Criterion 19.1* (Met) - Reporting entities in the IoM are required under para. 15(4) of the AML/CFT Code to apply enhanced CDD measures, proportionate to the risks, to business

relationships and occasional transactions with natural and legal persons (including FIs) resident or located in countries that are *subject to a FATF call to apply counter-measures in order to protect the international financial system from on-going and substantial ML/TF risks* (jurisdictions in "List A" which is maintained by the DHA).

222. *Criterion 19.2* (Met) - The IoM is able to apply a number of countermeasures when called upon to do so by the FATF and independently of any call by the FATF to do so. For example, the IOMFSA is able to use its licensing policy to prevent branches of companies established outside the IoM operating in the IoM, and rule 7.8 of the FSRB requires regulatory consent to acquire or establish a trading subsidiary, branch or representative office outside the IoM. The TOCFR Act 2014 also allows the Treasury to direct that business should be limited or ceased with a person carrying on business in a particular country, the government of that country, a person resident in that country, or a body corporate that is a subsidiary of such a person. In all cases, the IOMFSA and Treasury can take risk into account in decision-making.

223. *Criterion 19.3* (Met) - The IoM ensures that FIs are advised of concerns about weaknesses in the AML/CFT systems of other countries through the publication by the DHA on its website of relevant lists of countries specified in para. 15 of the AML/CFT Code. When any update is made to any of the lists ("List A" and "List B" - jurisdictions with strategic AML/CFT deficiencies or those considered to pose a higher risk of ML/TF - are relevant here), this is communicated to industry by the IOMFSA using a mail merge. The revised list is also published on the DHA and IOMFSA websites with an associated press statement.

Weighting and Conclusion

224. The IoM meets all of the criteria. **R.19 is rated compliant**.

Recommendation 20 – Reporting of suspicious transaction

225. In the 2009 Report, the IoM was rated largely compliant with R. 13 and partially compliant with SR IV. Reference may be made to paras. 632 to 648 of the 2009 Report. It was recommended that the FIU and supervisory authorities should take steps to enhance the timeliness of reporting of suspicious transactions, both in the case of ML and TF, and that legislation should be amended to provide comprehensively that suspicious attempted transactions must be reported promptly to the FIU. In relation to TF, it was established that legislation should be amended to address the deficiencies in the scope of ATCA, thereby providing the required scope of coverage for reporting.

226. Since the adoption of the 2009 Report, it is now provided specifically in sec. 153 and 154 of POCA 2008 that SARs should be made to the FIU "as soon as is practicable". The same wording is found in the POCML 2010, POTFC 2011 and MLTF 2013. Moreover, under the definition of ML in sec. 158(11) of the POCA 2008, an attempt to commit a ML offence is now subject to suspicious transaction reporting in the same way as an offence that has been committed. In addition, the POCML 2010 and the POTFC 2011 also explicitly refer to suspicious attempted transactions. Reference is also made in the MLTF 2013 to knowledge or suspicion of attempted ML or attempted TF.

227. The ATCA 2011, which came into effect on 13 July 2011, extends the definition of terrorism to include all offences as defined in the nine Conventions and Protocols listed in the Annex to the Financing of Terrorism Convention. The required scope of coverage for STR reporting is therefore being met.

228. *Criterion 20.1* (Met) - The obligation for FIs to report suspicions relating to funds that are proceeds of criminal activity[80] or funds that are related to TF is set out in POCA 2008 (sec. 142 to

[80] Criminal activity refers to all criminal acts that would constitute a predicate offence for ML in the IoM (See R. 3, c.3.2).

144, 153 and 154) and the ATCA (sec. 11, 12, 14 and 15). The disclosure regime is not based on a direct requirement to report suspicious activity, but on the criminalisation of the failure to disclose, together with statutory protection against legal action for making the disclosure, provided that certain conditions are met. The disclosure regime is an activity-based (SAR) one rather than a transaction-based one (STR) and relates to knowledge or suspicion of ML or TF. The evaluation team agrees with the conclusion of the 2009 Report that "in practice, the inverted nature of the STR reporting is considered to have the same meaning in law as a direct formulation and does not appear to impact negatively on the decision-making by FIs on whether or not to file a SAR with the FIU". In addition, paras. 27 and 28 of the AML/CFT Code require FIs and DNFBPs to have policies and procedures related to disclosure to the FIU when they know or suspect or have reasonable grounds for knowing or suspecting that another is engaged in ML/TF.

229. *Criterion 20.2* (Met) - The obligation to report, albeit an indirect obligation, covers all suspicious transactions (regardless of the amount). Moreover, as highlighted above, suspicious attempted transactions are also covered.

Weighting and conclusion

230. The IoM meets all criteria under R.20. **R.20 is rated compliant**.

Recommendation 21 – Tipping-off and confidentiality

231. In the 2009 Report, the IoM was rated partially compliant with R. 14. Reference may be made to paras. 649 to 655 of the 2009 Report. The measures recommended in the 2009 Report were addressed through the introduction of new provisions in the POCA 2008 and other legislation.

232. *Criterion 21.1* (Met) - Under sec. 153 of the POCA 2008 any person making a disclosure in the course of his trade, profession, business or employment is not to be taken to breach any restriction on disclosure of information (however imposed), provided that certain conditions set out in the law are met. This provision covers disclosures made to the FIU in good faith by FIs, and, although no specific reference is made to directors, officers and employees of a FI, these categories of persons would also fall within the scope of the provision. The wording of the law does not specifically mention that there is a protection from criminal and civil liability; however, the fact that no breach of any restriction on disclosure of information would arise has the same legal effect. Moreover, once these disclosures are based on knowledge or suspicion, the protection is considered to be available even if the discloser did not know precisely what the underlying criminal activity was, and regardless of whether illegal activity actually occurred.

233. A similar provision in ATCA (sec. 15) applicable to persons in the regulated sector provides a similar level of protection as that provided under sec. 153 of POCA 2008.

234. *Criterion 21.2* (Mostly met) - FIs, their directors, officers and employees are prohibited by law from disclosing the fact that a disclosure has been made to the FIU. The relevant provision is sec. 145 of POCA 2008 which states that any person who discloses to third parties the fact that a disclosure has been made to the FIU commits a criminal offence. For the tipping-off provision to apply, however, the disclosure to third parties must be 'likely to prejudice any investigation that might be conducted' following the disclosure to the FIU. The effect of this limitation is that the likelihood of prejudice to an investigation would not necessarily be as broad a prohibition as required by R. 21. This is further demonstrated by sec. 148(3), according to which a person is excused from being held accountable if he/she did not know or suspect that the disclosure would prejudice an investigation. Sec. 27 of ATCA contains similar provisions to sec. 160 of POCA 2008, but in relation to terrorist investigations (which include terrorist financing investigations – sec. 19 of ATCA). However, it appears that, unlike the provisions contained in sec. 145 of POCA 2008, ATCA only contains provisions prohibiting tipping-off in situations where a person knows or has reasonable cause to suspect that a constable is conducting, or proposes to conduct, a terrorist

investigation, and not in situations where disclosure is likely to prejudice any investigation that might be conducted following the disclosure.

Weighting and conclusion

235. The IoM meets c.21.1 and mostly meets c.21.2. **R.21 is rated largely compliant**.

Recommendation 22 – DNFBPs: Customer due diligence

236. In the 2009 Report, the IoM was rated partially compliant with these requirements (see paras. 781-839). The deficiencies related to concerns over implementation of CDD measures by accountants, inconsistencies in legislation with regard to the CDD exemptions in the case of CSPs and TSPs, and concerns about effectiveness of implementation of the supplemental provisions of the AML Code 2008. Since then, the IoM has: (i) consolidated ML and TF requirements into a new AML/CFT Code which provides a single legal text for preventive measures to be applied by all FIs and DNFBPs listed in Schedule 4 of the POCA 2008[81], excluding online gambling; and (ii) Online Gambling Code which came into force in May 2013 and replaced previous versions of Online Gambling Codes.

237. *Criterion 22.1* (Mostly met) - See R.10 (CDD) for a description of these requirements (which applies to all DNFBPs except for online gambling operators). In addition, online gambling operators are required to comply with the CDD requirements of the Online Gambling Code and the following paras. outline only deficiencies.

238. Although, the Online Gambling Code requires the licensee to have regard to the value of funds deposited, there is no mandated threshold for evidence of identity to be obtained on the placing of a deposit (though the GSC suggests in guidance that the identity of a participant should be verified when deposits equal or exceed EUR 3 000 within the space of a month). Also, there is no clear requirement in the Online Gambling Code to apply CDD measures where there is doubt about previously obtained data or suspicion of ML/TF.

239. Para. 9(2)(c) and (d) of the Online Gambling Code requires a business (corporate) participant to verify that any person purporting to act on behalf its behalf is authorised to do so and to take reasonable steps to verify the identity of that person (which is different to the standard which requires identity to be verified and does not refer to "reasonable steps"). Whilst there are no similar requirements for participants who are individuals, Reg. 5(1) of the Online Gambling (Registration and Accounts) Reg. 2008 is intended to preclude the use of agents and proxies playing on an online platform on behalf of another individual.

240. The definition of "beneficial owner" in the Online Gambling Code is deficient since it means only the natural person who ultimately owns or controls a business participant, and not also the natural person on whose behalf a transaction is being conducted. This means that it is not necessary to identify or verify the identity of players that place bets through another gambling operator (known as a "business to business" relationship). Also, there are no specific requirements in the Online Gambling Code for the identification and verification of individuals related to trusts or other types of legal arrangement, though GSC AML/CFT Guidance does provide details on how participants that are legal persons or legal arrangements should be identified and verified, in particular with respect to owners and controllers of that legal person or legal arrangement.

241. Para. 11 of the Online Gambling Code (on-going monitoring) does not require reviews of existing records (to ensure that they remain up to date) to take account of risk.

242. There is no specific requirement in the Online Gambling Code to understand the nature of a participant's business, to collect an address, to collect proof of existence, or to collect information

[81] Amended in April 2015 to include some further designated business, e.g.: virtual currency operators; provision of safe custody facilities; and Specified Non-Profit Organisations.

on powers that regulate and bind a participant. However, GSC AML/CFT Guidance provides further details on how participants that are legal persons or legal arrangements should be identified and verified, including verification of existence and information on the registered address.

243. The Online Gambling Code does not include a clear requirement for CDD measures to be applied to existing participants.

244. Para. 6(3) of the Online Gambling Code requires an online gambling operator to comply with para. 10 (enhanced due diligence) in respect of a participant or business participant that has been assessed as posing a higher risk. This must always include taking reasonable measures to establish source of funds and source of wealth. However, it is only necessary to consider taking other measures, e.g. enhanced on-going monitoring (and not to actually apply those measures).

245. There is no provision that allows an online gambling operator not to perform CDD if this would result in the participant being tipped off.

246. *Criteria 22.2 (R.11)* (Mostly met) - See R.11 (record-keeping) for a description of these requirements (which applies to all DNFBPs except for online gambling operators). In addition, paras. 12 and 13 of the Online Gambling Code require: (i) all records of transactions to be kept for a period of 6 years after the person concerned ceases to be a participant; and (ii) records obtained through CDD measures to be kept indefinitely (since no period is specified). However, online gambling operators are not required to keep account files and business correspondence with customers.

247. *Criteria 22.3 (R.12)* (Partly met) - See R.12 (PEPs) for a description of these requirements (which apply to all DNFBPs except for online gambling operators. In addition, para. 6 of the Online Gambling Code does not include a requirement: (i) to put in place risk management systems to determine whether a participant or the beneficial owner is a PEP; or (ii) to obtain senior management approval before establishing or continuing such business relationships. Nor are domestic PEPs covered by legislation, although the GSC's AML/CFT Guidance recommends online gambling operators to identify domestic PEPs and undertake the appropriate level of risk management.

248. *Criteria 22.4 (R.15)* (Mostly Met) - See R.15 (new technologies) for a description of these requirements (which apply to all DNFBPs except for online gambling operators. In addition, para. 20 of the Online Gambling Code requires an online gambling operator to establish, maintain and operate appropriate procedures and controls for preventing the misuse of technological developments for the purposes of ML/TF. GSC AML/CFT Guidance provides further details on risk assessments associated with technological developments and advises online gambling operators to conduct risk assessments every time money and technology come together in a new way. Guidance however, is not an enforceable mean. There is no requirement to identity and assess risks that may arise in relation to the development of new products and new business practices (though such risks will be identified where new or developing technology is used). Nor is the timing of the application of procedures and controls specified.

249. *Criteria 22.5 (R.17)* (Mostly met) - See R.17 (reliance on third parties) for a description of these requirements (which apply to all DNFBPs except for online gambling operators). Reliance on third parties is not permitted under the Online Gambling Code.

Weighting and conclusion

250. The IoM mostly meets c.22.1, 22.2, 22.4 and 22.5 and partly meets c.22.3. **R.22 is rated largely compliant**.

Recommendation 23 – DNFBPs: Other measures

251. In its 2009 Report, the IoM was rated partially compliant with these requirements (see paras. 840 to 859). The deficiencies related to the absence of a requirement to report attempted suspicious transactions and the absence of clear legal requirement to maintain an adequately resourced and independent audit function to test compliance with AML/CFT procedures in line with the nature, size and activity of the DNFBP. The legal protection for those reporting suspicions was not fully in line with the international standard and there were some concerns about the effectiveness.

252. *Criterion 23.1* (R.20) (Met) - See R.20 (reporting of suspicious transactions) for a description of these requirements.

253. *Criterion 23.2* (R.18) (Partly met) - See R.18 (internal controls and foreign branches and subsidiaries) for a description of these requirements (which apply to all DNFBPs except for online gambling operators). Also, online gambling operators are required to establish, maintain and operate procedures and controls under para. 4 of the Online Gambling Code that include: (i) screening procedures (para. 18); (ii) on-going training (para. 19); and (iii) procedures for monitoring and testing compliance with ML/TF requirements. However, with the exception of (iii), there is no requirement that such procedures and controls have regard to ML/TF risks or the size of the operator. Nor is there is a requirement to appoint a compliance officer or to have an independent audit function to test the system.

254. There is no specific requirement in the Online Gambling Code to have group-wide programmes against ML/TF for online gambling. Nor does the Online Gambling Code contain any specific requirement for branches and majority-owned subsidiaries of an online gambling operator.

255. *Criterion 23.3* (R.19) (Mostly met) - See R.19 (higher risk countries) for a description of these requirements (which apply to all DNFBPs except for online gambling). Also, para. 6 of the Online Gambling Code requires an online gambling operator to apply enhanced CDD with natural and legal persons resident or located in a country that the licence holder has reason to believe does not apply, or insufficiently applies, the FATF Recommendations (which is bound to include countries which are the subject of a FATF call for application of enhanced measures). Whilst there are no measures in place to actively advise online gambling operators of any concerns about weaknesses in the AML/CFT systems of other countries, the GSC expect operators to use publicly available assessments, including the FATF's own list of high-risk and non-cooperative jurisdictions, and the use of "List A" and "List B" published by the DHA is covered in sec. 5.2 of the GSC AML/CFT Guidance. With respect to the more general application of countermeasures, the TOCFR Act applies also to online gambling operators.

256. *Criterion 23.4* (R.21) (Mostly met) - See R.21 (tipping off and confidentiality) for a description of these requirements.

Weighting and conclusion

257. The IoM meets c.23.1, mostly meets c.23.3 and 23.4, and partly meets c.23.2. **R.23 is rated partially compliant**.

Recommendation 24 – Transparency and beneficial ownership of legal persons

258. In the 2009 Report, the IoM was rated largely compliant with former R.33. Since then, the FATF standard has changed substantially. In previous report the assessors identified as a deficiency that for about 30 per cent of the companies incorporated under Companies Act 1931 to 2004 (1931 Companies) and limited liability companies incorporated under the Limited Liability Companies Act 1996 (LLCs), it could not be determined that accurate, complete, and current beneficial ownership information was available.

259. General partnerships and limited partnerships (including those with a legal personality) established under the Partnership Act 1909 are considered under R.24. Sec. 22 of the Partnership Act says that all property and rights and interests in property originally brought into the partnership stock or acquired, whether by purchase or otherwise, on account of the firm or for the purposes and in the course of the partnership business are called "partnership property", and must be held and applied by the partners exclusively for the purpose of the partnership and in accordance with the partnership agreement. Sec. 23 of the same Act says: Unless the contrary intention appears, property bought with money belonging to the firm is deemed to have been bought on account of the firm.

260. *Criterion 24.1.* (Mostly met) - Information on the various types, forms and basic features of IoM legal persons is found in the relevant laws[82], which are publicly available via the IoM Government Online Legislation website and Central Registry[83]. In addition, the authorities publish a number of guides. The Department for Economic Development publishes guides (http://www.whereyoucan.com/fiduciaries) explaining the forms and basic features of 1931 companies, companies incorporated under the Companies Act 2006 (2006 companies), LLCs and limited partnerships, and the Companies Registry publishes a number of practice notes, covering 1931 companies, 2006 companies, LLCs, foundations and partnerships. However, these guides and practice notes do not explain, or do not fully, explain the process followed for obtaining and recording beneficial ownership information.

261. *Criterion 24.2*. (Mostly met) - To date, there has not been a formal assessment of the particular threats that may be presented by use of each of the above listed legal persons informed by typologies involving legal persons established under Manx legislation. Instead, relevant recognised international typologies for legal persons were referred to in order to identify generally how legal persons established in the IoM could be used in ML/TF (without taking account of any particular distinguishing factors of Manx legal persons, or between different types of legal person). In addition, as part of the NRA, the authorities have considered: (i) the availability of, and access to, beneficial ownership information for 1931 companies, 2006 companies and LLCs (but not also limited partnerships and foundations - use of which is limited) and have identified a number of vulnerabilities (and set actions to address these vulnerabilities); and (ii) vulnerabilities in the current legislative framework to regulate legal persons.

262. *Criterion 24.3*. (Mostly met) - All types of company are required to register with the Central Registry. The Registrar certifies that a company is incorporated under sec. 13(1) of the Companies Act 1931 to 2004; sec. 8 of the Limited Liability Companies Act 1996; and sec. 3(1) of the Companies Act 2006. There is a public register of all such companies which contains "basic information" in line with c.24.3[84]. This information may be inspected under sec. 284A of the Companies Act 1931 to 2004, sec. 209 of the Companies Act 2006, and sec. 48 of the Limited Liability Companies Act 1996. However, sec. 204 of the Companies Act 2006 allows a company to elect not to file a copy of its register of directors with the Central Registry. Whilst details of directors must be provided as part of its annual return, this information could be up to a year out of date.

263. Whilst there is no register of general partnerships, the IoM does keep a publicly available and searchable list of business names, which includes general partnerships not operating under their registered name. Where general partnerships register their business name, they must list all names and residential addresses of all partners, and the address of the principle place of

[82] Companies Act 1931 to 2004, Limited Liability Companies Act 1996, Companies Act 2006, Foundations Act 2011, and Partnership Act 1909.

[83] http://www.legislation.gov.im/cms/en/ and https://www.gov.im/categories/business-and-industries/companies-registry/acts-and-regulations/

[84] In the case of a LLC, there is a register of members of the LLC who participate in its management in proportion to their contribution to the capital of the company.

business. Every limited partnership must be registered with the Central Registry. Basic information listed in line with c.24.3 about limited partnerships may be inspected through the Central Registry under sec. 58 of the Partnership Act 1909, except that a limited partnership is not required to register its partnership deed.

264. To establish a foundation, the Registrar must enter prescribed information in the Central Registry in accordance with sec. 34 of the Foundations Act 2011. Sec. 48 of this Act allows basic information in line with c.24.3 to be inspected, except that a foundation is not required to register its rules (distinct from the foundation instrument) with the Central Registry. It is these rules that describe the foundation's basic regulating powers.

265. Members of the public can also see and order copies of all statutory documents held about a company, foundation or limited liability partnership at the Central Registry at a nominal cost (GBP 2 for one document or GBP 15 for all documents). This can be done on-line (https://services.gov.im/companies-registry/) or in person at the Central Registry.

266. *Criterion 24.4.* (Mostly met) - 1931 companies are required to keep registers of directors and members in the IoM under sec. 143 and 96 of the Companies Act 1931 to 2004 respectively (at the registered office or other address notified to the Central Registry). However, there is no direct requirement for 1931 companies to keep a copy of the company's memorandum and Art. (which hold information on company name, legal form and status, registered office address, and basic regulating powers) or proof of incorporation. The register of members must contain a "statement" on the shares held by each shareholder (including number and class). Voting rights need not be contained in these registers but will be set out in the constitution documents.

267. Inter alia, 2006 companies are required to keep the following documents under sec. 78 and 79 of the Companies Act 2006: (i) copies of memorandum and Art. (which hold information on company name, legal form and status, registered office address, and basic regulating powers); (ii) register of directors or a copy of the register of directors; (iii) register of members; and (iv) copies of all resolutions consented to by directors and members to amend the memorandum and Art. This information must be held by a registered agent (at an address in the IoM notified to the Registrar) or (in the case of resolutions) by the company itself (inside or outside the IoM). Under sec. 62(1), the register of members must contain details of the number and class of shares held by each shareholder. Voting rights need not be contained in these registers but will be set out in the constitution documents. Whilst there is no requirement to hold proof of incorporation, this must be held by the registered agent under the AML/CFT Act (though not necessarily in the IoM).

268. Inter alia, the following information must be included in a LLC's Art. of organisation under sec. 7 of the Limited Liability Companies Act 1996: (i) name; (ii) names and addresses of members[85] (which manage the company like partners in a partnership); and (iii) basic regulating powers. Whilst the LLC's legal form and status will be clear from the Art., there is no requirement to hold proof of registration or information on registered office address, nor for the Art. of organisation to be held in the IoM (though each change must be reported by the registered agent to the Central Registry within one month). As a result of CDD requirements in the AML/CFT Code, the registered agent must hold this information and documents (as the LLC is its customer), though not necessarily in the IoM.

269. A foundation must keep the documents and records specified in sec. 41(2) of the Foundations Act 2011 at its business address or at such other place, within or outside the IoM. These include: (i) a copy of its foundation instrument and foundation rules (which hold information on foundation name, legal form and status, registered office address, and basic regulating powers); and (ii) a register showing the names and addresses of the members of its council. There is no requirement under the Act for: (i) proof of registration; or (ii) information on founders,

[85] Where there is any change in the membership of a LLC, sec. 7(3)(c) of the Limited Liability Companies Act 1996 requires its Art. of organisation to be amended.

enforcers or known beneficiaries to be held. Despite this, proof of registration and other information will be held by a registered agent about the foundation (its customer) in the IoM (as a result of CDD requirements in the AML/CFT Code), though not necessarily in the IoM.

270. Whilst the general partner of a limited partnership (incorporated or otherwise) is implicitly required by virtue of sec. 50 and 51 of the Partnership Act 1909 to maintain a record of information set out in c.24.3 and of limited partners – there is no requirement for this information to be held in the IoM. However, information about general and limited partners is held at the Central Registry. No requirements are placed by statute on general partnerships to hold information set out in c.24.3 and c.24.4.

271. *Criterion 24.5.* (Partly met) - Companies, limited partnership and foundations are required to notify the Central Registry about most changes within one month of their occurrence. These changes are a matter of public record. Whereas legal persons will be aware when there is a change of information set out in c.24.3 (as they must adopt the change), they will not necessarily be aware when there is a change in legal ownership of shares in a 1931 company or 2006 company. However, entry of the name of a person in the register of members as a holder of a share in a company is prima facie evidence that legal title in the share vests in that person (sec. 69 of the Companies Act 1931 and sec. 63(1) of the Companies Act 2006). In the case of a LLC[86], any changes in ownership must be agreed by members. Where a partnership registers a business name, any change in information notified at the time of registration must be disclosed to the Central Registry within one month of the change taking place.

272. The Central Registry is a repository of information and accepts submissions that are prescribed by statute in good faith. Accordingly, it does not check the accuracy of information provided. However, companies must submit an annual return of basic information (including shareholders) to the Central Registry, which then checks that information in the return is consistent with what is already on the Registry's files. If it is not, then the Registrar follows this up. If this annual return is not submitted within the prescribed filing period the Registry has powers to take action to remove it from the register (sec. 273 of the Companies Act 1931 to 2004, sec. 183 of the Companies Act 2006, sec. 11 of the Limited Liability Companies Act 1996, and sec. 51A of the Partnership Act 1909). Foundations are also required to submit annual returns. Whilst there are no similar strike-off provisions (on the basis that this would leave any assets in limbo and disadvantage the beneficiaries), the Registrar would refer a matter of failing to submit a return to the Attorney General for action under sec. 44 of the Foundations Act 2011.

273. The Central Registry does not ensure that information recorded by legal persons on categories of shares (including the nature of associated voting rights) is accurate and updated on a timely basis.

274. *Criterion 24.6.* (Partly met) - The IoM uses two mechanisms to obtain beneficial ownership information for companies and foundations: (i) appointment of a nominated officer; or (ii) appointment of a registered agent.

275. 1931 companies are required to appoint a nominated officer under the CBO 2012 who is resident in the IoM. That person must be: (i) an individual (not subject to the AML/CFT Code); or (ii) TCSP that is licenced by the IOMFSA to carry on corporate services (and so subject to the AML/CFT Code). They are not required to also appoint a registered agent (though the authorities have explained that, in 2014/15, just over half of the companies incorporated under the Companies Act 1931 to 2004 were serviced by TCSPs in some way). Details of the nominated

[86] The interest of members may be transferred or assigned as provided in the operating agreement. If all the members of a LLC other than the member proposing to dispose of his interest do not approve of the proposed transfer or assignment by unanimous written consent, the transferee of the member's interest shall have no right to become a member of the limited liability company; or to participate in the management of the business and affairs of the limited liability company.

officer must be notified by the company to the Central Registry within one month of appointment and any subsequent change of officer or change in details must also be disclosed within one month of the date of the change. Information on a company's nominated officer is also collected in the annual return delivered to the Central Registry, which is a matter of public record.

276. Under sec. 7 of the CBO 2012, a statutory obligation is placed on each registered member of a company (individual or legal person) that is not also the "beneficial owner" to provide the nominated officer with details of the beneficial owner of the shares. "Beneficial owner" means the person (not individual) ultimately beneficially interested in the membership interest and may be traced through any number of persons or arrangements. The extent of beneficial ownership information to be provided to the nominated officer depends on: (i) the legal status of the beneficial shareholder (individual or legal person); and (ii) number of beneficial owners.

277. In a case where the beneficial owner of registered shares is an individual or legal person, the registered shareholder must provide prescribed details of that person to the nominated officer within 3 months of the registered shareholder becoming a member of the company. In a case where a legal person is the beneficial owner, it is not also necessary to provide information on the beneficial ownership of that legal person. The authorities have said that a legal person may be a beneficial owner where it has no beneficial owner, e.g. a foundation, but this explanation is inconsistent with the AML/CFT Code (under which a foundation does have beneficial owners) and means that insufficient information may be held to show who is the beneficial ownership (as understood under c.24.6) of the company. In a case where the class of beneficial owners is of such a size that it is not reasonably practicable to identify each member of the class (a term that is not explained in guidance), the registered shareholder must provide details that are sufficient to identify and describe the class of persons who are the beneficial owners.

278. The nominated officer is not required to hold on to beneficial ownership information that is provided in accordance with the law. Nor are all companies required to appoint a nominated officer: there are exemptions under: (i) CBO 2012, e.g. a company that is listed on a recognised exchange or which is a collective investment scheme; and (ii) the Companies (Beneficial Ownership)(Exemptions) Order 2013[87]. Not all of these exemptions appear to be in line with the standard.

279. For other types of legal person (except limited partnerships with legal personality), a registered agent must be appointed under sec. 74 of the Companies Act 2006, sec. 5 of the Limited Liability Companies Act 1996 or sec. 28 of the Foundations Act 2011. In the case of a 2006 company and foundation, the registered agent must be a person that is licenced by the IOMFSA to carry on corporate services. In the case of a LLC, the Limited Liability Companies (Registered Agents' Qualification) Regulations 2003 do not include a similar restriction, though the effect of the RAO 2011 will be to require such an agent to hold a class 4(5) licence where the agent is acting by way of business. Accordingly, this is not considered to be a shortcoming. Under the AML/CFT Code, the registered agent will be required to: (i) identify the beneficial owner and take reasonable measures to verify the identity of any beneficial owner of the customer, using relevant information obtained from a reliable, independent source; and (ii) hold records.

280. A limited partnership must maintain a place of business in the IoM but is not required to have a registered agent or to hold information on beneficial ownership at that place of business. No mechanisms are in place to ensure that information on the beneficial ownership of a general partnership is obtained and available at a specified location.

281. In the particular case of collective investment schemes, including those with a limited number of investors, whilst para. 21 of the AML/CFT Code allows fund functionaries (class 3 licence

[87] This includes: public companies (i.e. companies not prohibited by their Articles from inviting the public to subscribe for any shares or debentures of the company); registered charities; companies promoting art, science, sport, commerce, charity or any profession; and entities licensed by the IOMFSA or GSC.

holders) to refrain - in defined circumstances - from finding out and verifying the identity of third parties on whose behalf an investor may be acting, this exemption may not be applied by the scheme itself, which is responsible for performing CDD on its investors, or by the scheme's registered agent. The effect of this is that information on the ultimate beneficial ownership of such schemes must be obtained and would be available through regulated functionaries or the registered agent.

282. *Criterion 24.7.* (Partly met) **-** Under sec. 7(4) of the CBO 2012, a member of a 1931 company must notify the nominated officer within three months of any change in beneficial ownership of the company (but see deficiencies highlighted under c.24.6). This period is significantly longer than the time that is given to a company to notify the Central Registry of a change in legal ownership. Whilst this may reflect the different status of the person on whom the obligation is set (a 1931 company is regulated whereas its shareholders are not), three months is considered by evaluators to be too long a period. It is an offence for a shareholder not to notify a change or to make a statement to the nominated officer which is false, deceptive or misleading, and may be punished, following a trial, on summary conviction (by the Summary Court) by a fine not exceeding GBP 5 000 or otherwise (by the Court of General Gaol Delivery) by an unlimited fine.

283. In the case of a registered agent, para. 9(1)(a) of the AML/CFT Code requires it to perform on-going monitoring of every business relationship, including reviews of information held for the purposes of CDD to ensure that it is up-to-date and appropriate (in particular where a relationship poses a higher risk of ML/TF). Compliance with this requirement is assessed under c.10.7 and supervision of compliance with this requirement by TCSPs is considered under R.28. Since the mechanism used (using information obtained by TCSPs in accordance with R.22) is one that is recognised under c.24.6, assessors consider this to be a sufficient basis for ensuring that beneficial ownership information is accurate and as up to date as possible.

284. As noted under c.24.6, no mechanisms are in place to ensure that information on the beneficial ownership of a partnership is obtained.

285. *Criterion 24.8.* (Mostly met) - In the case of 1931 companies, the nominated officer must disclose, in accordance with any notice given, information the officer holds in respect of the beneficial ownership of the company specified or referred to in the notice. The nominated officer commits an offence if they, without reasonable excuse, fail to comply with the notice or make a statement, in response to receiving a notice, which is false, deceptive or misleading. In the case of basic information, the authorities have not explained what measures are used to ensure that companies cooperate with competent authorities to the fullest extent possible.

286. Registered agents are subject to: (i) licensing criteria applied by, and powers available to, the IOMFSA; and (ii) rule 8.3 of the FSRB which mandates compliance with "regulatory requirements". The effect of both will be to require registered agents to give further assistance to all competent authorities where information is requested in accordance with statutory requirements. In addition, sec. 43 of the FSA 2008 permits the IOMFSA to take action for breach in respect of a licence holder which contravenes any statutory provision.

287. The authorities have not provided information on how it is ensured that partnerships cooperate with competent authorities.

288. *Criterion 24.9.* (Partly met) - There are no requirements under CBO 2012 for a nominated officer to maintain information and records after a 1931 company has been dissolved or otherwise ceases to exist. Otherwise, the disposal of "books and papers" (including basic information) of a wound-up company is covered by the Companies Act 1931 to 2004. Under sec. 266 (which applies also to 2006 companies and may also (but need not) be applied "unregistered

companies"[88]), the person charged with keeping records will be "responsible" for their destruction if they are not retained for a period of 5 years post dissolution unless the Court or committee of inspection or creditors direct otherwise. However, it is not clear what the extent of this responsibility is, and how it will be enforced. In any event, sec. 266 does not set a direct requirement to keep records; nor is an offence committed where records are not kept. There are no specific provisions dealing with the retention of books or records in the case of a company that is struck-off, dissolved (simplified process), continued into another company, or merged with another company. No record keeping requirements are placed on a foundation that is dissolved.

289. In addition, a registered agent will be required to maintain information and records for at least 5 years after the day on which the customer ceases to be a customer.

290. As noted under c.24.6, no mechanisms are in place to ensure that information on the beneficial ownership of a partnership is obtained.

291. *Criterion 24.10*. (Met) Competent authorities have all the powers necessary to obtain timely access to basic and beneficial ownership information, including from registered agents. This is explained under c.27.3 (which is relevant to TCSPs) (IOMFSA), c.29.3 (FIU) and c.31.1 (law enforcement). In the case of 1931 companies, the nominated officer must disclose beneficial ownership information in accordance with a notice that may be given by: the Attorney General; Chief Constable; officer of the Financial Crime Unit of the IoM Constabulary (FCU); the IOMFSA; Assessor of Income Tax; Collector of Customs and Excise; or any person appointed by any of these persons.

292. *Criterion 24.11.* (Met) - Historically, it has been possible for 1931 companies and 2006 companies to issue bearer shares. However, the Companies, etc. (Amendment) Act 2003 amended the Companies Act 1931 to 2004 to provide that, from 1 April 2004, no new bearer shares could be issued by companies incorporated under that law and the rights relating to existing bearer shares could not be exercised until those shares were registered by the company. Sec. 30 of the Companies Act 2006 also prohibits the issue or creation of new bearer shares by companies incorporated under that Act and makes any attempt to do so an offence. Moreover, the Companies (Prohibition of Bearer Shares) Act 2011 came into effect on 12 October 2011. As a result, any company with bearer shares in issue on that date had until 12 April 2012 to convert those shares into registered shares. Sec. 70A & 70B of the Companies Act 1931 to 2004 and sec. 30 and 218 of the Companies Act 2006 address bearer shares, the definition of which specifically includes a bearer warrant.

293. *Criterion 24.12.* (Partly met) - The concept of a "nominee" director does not exist in IoM law. In line with a definition in sec. 21(1) of the Company Officers (Disqualification) Act 2009, every director has an equal duty of responsibility to a company. A director who neglects that responsibility in the interests of, or on the orders of, a principal will be guilty of a breach of duty. Since this may not prevent directors acting on behalf of other individuals, the IoM introduced a regulatory regime in 2000 for directors that act by way of business, including "fit and proper" licensing of such directors (except those acting for 10 or less companies).

294. As explained under c.24.6, a registered shareholder of a 1931 company is required to disclose the name of its "nominator" to the company's nominated officer under the CBO 2012. However, this information is not also disclosed to the company or to the Central Registry to be included in the relevant register. Indeed, legislation may prevent disclosure of information on beneficial ownership since sec. 102 of the Companies Act 1931 to 2004 does not permit trusts to be entered on a register.

[88] An unregistered company includes a partnership, whether limited or not, any association and any company which consists of eight or more members.

295. More generally, acting, or arranging for another person to act, as a nominee shareholder or nominee member of a company or limited partnership by way of business is a regulated activity by virtue of Class 4 (Corporate Services) of the RAO 2011. Such a TCSP will be required to apply CDD measures under the AML/CFT Code which will include maintaining information identifying the nominator (the beneficial owner of shares). However, there is no requirement for: (i) nominees carrying on business outside the IoM to be licensed where they hold shares or interests in IoM companies or partnerships; nor (ii) the nominee status of shares or interests held by a TCSP to be recorded in the Central Registry. Thus, there is no transparency provided for FIs, DNFBPs and other parties doing business with the company who might seek to verify beneficial ownership information by requesting an extract of the shareholders' register or register held in the Central Registry.

296. The authorities have explained that there is no legal basis for someone to be a partner on a nominee basis. A person is either a partner and liable as such, or not a partner, under the Partnership Act 1909.

297. *Criterion 24.13.* (Mostly met) - In the case of a 1931 company, sec. 5(5) and 6(5) of the CBO 2012 make it an offence for a company to fail to appoint a nominated officer, keep records about that nominated officer, or provide information about the nominated officer to the Central Registry. Sec. 7(4) of the CBO 2012 makes it an offence for a registered shareholder to fail to disclose information on beneficial ownership to the nominated officer. Sec. 10(7) of the CBO 2012 makes it an offence for a nominated officer: (i) to fail to comply, without reasonable excuse, with a notice to provide information that is held; or (ii) make a statement, in response to receiving a notice, which is false, deceptive or misleading. Under sec. 13 of the CBO 2012, and following a trial, a person guilty of an offence under the CBO Act is liable on conviction to a fine not exceeding GBP 5 000.

298. Failure to comply with requirements set in other legislation regulating legal persons and partnerships can be punished by a "default" fine. One notable exception to this relates to failure to convert bearer shares to registered shares, where a person that is found guilty of an offence following a trial is liable to a custodial sentence not exceeding 2 years or to an unlimited fine, or to both.

299. Under sec. 41 of the AML/CFT Code, a registered agent who contravenes its requirements is guilty of an offence and following a trial liable on conviction to a custodial sentence not exceeding 2 years or to a fine, or to both. In addition, a registered agent that is a TCSP (the majority) that fails to act in a way expected by the IOMFSA will be subject to the full range of sanctions that is set out under c.35.1. The authorities have not provided information on partnerships.

300. Liability and sanctions for failing to grant to competent authorities timely access to information are explained at c.25.8 where it is noted that the range of sanctions that can be applied by the FIU and law enforcement is not considered to be proportionate (particularly in a case where an offence is committed by a legal person).

301. *Criterion 24.14.* (Met) - All of the relevant investigative measures outlined at R.37.1 can be applied in the event of a MLA request in relation to basic and beneficial ownership information. In addition to other sources considered, the requesting party is provided with the website address for the Central Registry, where basic information and a number of documents are publicly available (at the investigation stage and prior to an international LOR being issued). Information on shareholders held by the Central Registry can also be provided.

302. Where a request for information is received under an international arrangement and that request includes basic information held by the Central Registry as well as information held by third parties in the IoM which is not publicly available and which will require the use of the

competent authority's information gathering powers, an interim response is provided to expedite the provision of the public information.

303. Sec. 34(3) of the FSA 2008 (the scope of which covers TCSPs) allows the IOMFSA to exercise powers conferred on it by that Act for the purpose of investigating any circumstances referred to in a request from a regulatory authority with which the IOMFSA has a mutual assistance agreement[89], including obtaining beneficial ownership information[90]. Sec. 34(2) of the FSA Act also permits spontaneous exchange of information by the IOMFSA where it has a mutual assistance agreement with an overseas regulator. Furthermore, para. 2(5) of Schedule 5 permits the disclosure of information by the IOMFSA on request to an overseas regulatory authority where information disclosed relates to the IOMFSA's Reg. and supervision of persons undertaking regulated activities. It is difficult to think of any assistance that could not be provided based on these provisions.

304. Inter alia, sec. 10(4) of the CBO 2012 permits information to be requested on the beneficial ownership of a 1931 company for the purpose of: (i) a criminal or regulatory investigation which is being, or may be, carried on outside the IoM; and (ii) facilitating a determination of whether any such investigation or proceedings should be initiated or brought to an end.

305. The FCU is able to provide international cooperation in relation to basic and beneficial ownership information, but only to the extent that it relates to a criminal investigation, criminal proceedings or recovery of property. The FIU exchanges information with foreign FIUs in accordance with the Egmont Group principles or under the terms of the relevant MOU, irrespective of the nature of the counterpart FIU.

306. *Criterion 24.15.* (Partly met) - All outgoing requests for MLA are dealt with by the Legal Officer, International Cooperation, who reports to the relevant prosecutor when a response is received. Sometimes, the response is sent directly to the investigating officer who also reports to the relevant prosecutor. Chasing letters, or, if appropriate, emails, are sent if required. However, the authorities have not otherwise explained how the quality of assistance is monitored, except in the case of requests for cooperation under international tax arrangements.

307. The IOMFSA monitors the quality of assistance received from other countries under the IOSCO multilateral memorandum of understanding. Otherwise, as the number of outgoing requests is low, any issues or trends could be identified and dealt with as necessary. The GSC does not formally monitor the quality of assistance received from other countries. However, requests are all dealt with by the GSC's Director of Licensing and Compliance and volumes are low, meaning that any issues/trends could easily be identified and fed back accordingly.

Weighting and Conclusion

308. The IoM meets c.24.10, 24.11 and 24.14, and mostly meets c.24.1 to 24.4, 24.8, and 24.13. It partly meets c.24.5 to 24.7, 24.9, 24.12 and 24.15. R.24 is rated partially compliant.

Recommendation 25 – Transparency and beneficial ownership of legal arrangements

309. In the 2009 Report, the IoM was rated largely compliant with these requirements. It was found that for legal arrangements administered by trustees who are not covered by, or who are excluded or exempted from the licensing requirements of FSA 2008, it could not be determined that accurate, complete and current beneficial ownership information is available.

---

[89] The FSA is a full signatory to the IOSCO Multilateral Memorandum of Understanding and signatory to the IAIS Multilateral Memorandum of Understanding. The FSA has entered into 27 Co-operation Agreements under the EU's Alternative Investment Fund Managers Directive. In addition, the FSA has 40 regulatory and supervisory MOUs.

[90] Evaluators consider that sec. 34(3) of the FSA 2008 must be read as referring to a regulatory authority with which the FSA has a mutual assistance agreement. This is because Schedule 2 of the FSA derives its powers from sec. 15 and 34(2) of the FSA 2008 (and not also sec. 34(3)).

310. *Criterion 25.1* (Partly met) - (a) Where a person acts, or holds itself out as acting, as trustee by way of business, in or from the IoM, it will be subject to the requirements of the AML/CFT Code. As such, in line with sec. 5 of sector specific guidance for TCSPs in the AML/CFT Handbook, the trustee of an established trust will be required under para. 13(3)(c), (e) and (f) and para. 13(5) to identify: (i) co-trustee or any other controlling party; (ii) known beneficiaries (but not also classes of beneficiaries)[91]; (iii) the settlor "or other person by whom the legal arrangement is made or on whose instructions the legal arrangement is formed"[92]; (iv) other natural persons having power to direct the customer's activities (which would normally include a protector, enforcer, and any other party to whom dispositive powers have been conferred[93]); (v) persons who may impose binding obligations on the customer; and (vi) those persons who are to receive benefit from the trust. Whilst the authorities have explained that it will be necessary to obtain information on classes of beneficiaries (and to have the capacity to be able to establish the identity of any beneficiary in the future) in order to assess the risk of a business relationship or occasional transaction in respect of a trust (para. 7 of the AML/CFT Code) there is no explicit requirement to obtain and hold this information.

311. Whilst the definition of "beneficial owner" in para. 3 of the AML/CFT Code means the natural person who ultimately owns or controls the customer or on whose behalf a transaction or activity is being conducted, paras. 13(3)(c), (e) and (f) and 13(5) of the AML/CFT Code and guidance in the AML/CFT Handbook do not explain the additional measures that will be needed where a person identified is not an individual.

312. These requirements do not apply to the trustee of an express trust that is governed by the law of the IoM where the trustee is: (i) resident outside the IoM; or (ii) resident in the IoM but non-professional (i.e. not acting by way of business), e.g. acting for a charitable trust or family members or close friends. Accordingly, the authorities have considered whether there are particular cases that may go some way to implying that common law obligations exist in relation to such trustees. There are many cases relating to the duty of a trustee to disclose information to, and to act in the best interests of, beneficiaries and the requirement for a valid trust to have certainty of objects, all of which could by extension imply that a trustee would need to keep and to maintain up to date records of each of the beneficiaries. However, these cases stop short of imposing an express obligation on a trustee to keep particular information, to keep that information updated and/or to retain records of that information for a particular period (or at all).

313. Furthermore, the duties of a trustee relate only to beneficiaries and would not include holding information on the settlor or protector. In practice, in order to fulfil his or her duties properly and fully, a trustee is likely, wherever possible, to keep such records in relation to each of those parties and to ensure that they are kept up to date, but the authorities have not been able to find any case law which creates a common law duty to do so.

314. As such, as a matter of good practice, trustees resident outside the IoM and non-professional trustees in the IoM are likely to maintain records such as those required under c.25.1, but there is no legal obligation to do so or sanctions for non-compliance other than e.g. an action brought by a beneficiary for a breach of duty by the trustee.

---

[91] In line with sec. 5 of sector specific guidance for TCSPs in the AML/CFT Handbook, where a potential beneficiary (who may be part of a class) is merely an object of a power and at best only has a hope of benefiting from the trust at the discretion of the trustees at some time in the future, the TCSP would be also be expected to know the name of this individual.

[92] This is designed to capture "dummy" settlors. The glossary to the AML/CFT Handbook explains what a dummy settlor is and why one might be used.

[93] Whereas the effect of guidance in the AML/CFT Handbook may be to limit the collection of information to a protector who has dispositive powers, the authorities have explained that this is not intended and guidance will be clarified in this respect.

315. In the particular case of unit trusts, including those with a limited number of investors, Art. 21 of the AML/CFT Code allows the trustee of a unit trust (class 3 licence holders) to refrain - in defined circumstances - from finding out the identity of third parties on whose behalf a registered investor may be acting. This means that information on the beneficial ownership of such schemes need not be obtained upfront by the trustee. However, the effect of conditions and terms of business that must be in place under para. 21 of the AML/CFT Code means that the registered investor must supply information to the trustee immediately upon request and have applied CDD measures in line with IoM requirements. Accordingly, information on the ultimate beneficial ownership of such schemes could be obtained and would be available through the trustee (a regulated functionary).

316. (b) There is no explicit requirement in the Trustee Act 2001 or implicit common law obligation requiring trustees to hold basic information on regulated agents of, and service providers to, the trust. However, there is a requirement in sec. 22 of the Trustee Act 2001 which requires a trustee to monitor the performance of its agents.

317. (c) Professional trustees carrying on their business in, or from, the IoM are subject to the AML/CFT Code which requires records to be maintained, including information specified under this criterion, for at least 5 years after their involvement with the trust ceases (para. 33 of the AML/CFT Code). No similar provisions apply to the professional trustee of an express trust that is governed by the law of the IoM where the trustee is resident outside the IoM.

318. *Criterion 25.2* (Partly met) - Where the trustee is subject to the AML/CFT Code, it must ensure that information held pursuant to this Recommendation is kept up-to-date and appropriate (para. 9(1)(a)). However, this requirement does not apply to the trustee of an express trust that is governed by the law of the IoM where the trustee is: (i) resident outside the IoM; or (ii) resident in the IoM but non-professional. As explained under c.25.1, there is no implicit obligation in common law to keep accurate and up to date information.

319. *Criterion 25.3* (Partly met) - There is no general obligation placed on trustees to disclose their status when entering into a business relationship or conducting an occasional transaction with a FI or a DNFBP. However, every trustee that holds a licence to undertake Class 5 business is obliged by Rule 6.14 of the FSRB to disclose in its correspondence that it is licensed. In addition, in respect of a trust bank account, Rule 3.27 of the FSRB requires that the title of the account must show that it is held by the trustee in the capacity of trustee and identify the trust to which it relates. This is primarily for the purposes of ensuring proper protection for the trust money. However, these requirements apply only to professional trustees that are regulated and supervised by the IOMFSA and do not apply to all types of business relationship or occasional transaction (e.g. with investment advisors or managers and lawyers).

320. *Criterion 25.4* (Partly met) - Trustees are not prevented by law or other provisions from providing competent authorities with any information relating to a trust - where a request is made using a legal power or relates to a criminal matter. However, application of the common law duty of confidentiality in respect of client information may prevent a trustee providing information to a FI or DNFBP, upon request, about the trust where terms of business (agreed with the customer) do not expressly address this area. In practice, where information cannot be provided, the FI or DNFBP would be unable to comply with the AML/CFT Code and would be required to freeze the relationship with the trustee and consider terminating it. Whilst it would not be practical for a trustee to withhold providing information, there is nevertheless an impediment to providing FIs and DNFBPs with information about a trust.

321. *Criterion 25.5* (Met) - Competent authorities have all the powers necessary to be able to obtain timely access to information held by trustees and other parties. This is explained under c.27.3 (which is relevant to TCSPs) (IOMFSA), c.29.3 (FIU) and c.31.1 (law enforcement). These powers may also be exercised in respect of any trustee that is exempted from licensing.

322. *Criterion 25.6* (Met) - The IoM's ability to provide international cooperation in relation to trusts and other legal arrangements is described under c.24.14.

323. *Criterion 25.7* (Met) - Trustees owe a "duty of care" under the Trustee Act 2001, reflecting the long established common law principle that trustees will act in the best interests of the trust. Accordingly, they can be held legally liable and sued in their capacity as trustee for failure to discharge duties, and this makes them vulnerable to civil action. The Trustee Act does not provide specific criminal penalties for failing to meet this duty of care, though fraud by a trustee is a criminal offence.

324. Where a trustee is subject to the AML/CFT Code, failure to comply with that Code will also be subject to sanctions which are explained under R.35. These can be applied proportionately. Where a trustee fails to disclose in correspondence that it is licensed or title of a bank account does not show that it is held by the trustee in the capacity of trustee and identify the trust to which it relates (both contraventions of the FSRB), the IOMFSA may undertake action for breach under sec. 19(1) of the FSA 2008. The list of powers covered by "action for breach" is set out at sec. 48(3) of the FSA 2008 and can be applied proportionately.

325. *Criterion 25.8* (Mostly met) - A person that fails to grant timely access to the IOMFSA is, in addition to administrative sanctions, liable, following a trial, on conviction to a custodial sentence not exceeding 2 years, or an unlimited fine, or both. A person that fails to grant timely access to the FIU is liable on conviction to a custodial sentence not exceeding 2 years, or to a fine not exceeding GBP 5 000, or to both. Whilst there is no offence for failing to comply with a production order (an order to produce material), failure to comply with a disclosure order (an order to answer questions, provide information or produce documents) is liable on conviction to custodial sentence not exceeding 6 months, a fine not exceeding GBP 5 000, or both. Under ATCA, failure to comply with a financial information order shall be liable on conviction to a fine not exceeding GBP 5 000.

326. In the case of the FIU and law enforcement, the range of sanctions that can be applied is not considered proportionate (particularly in a case where an offence is committed by a legal person).

Weighting and Conclusion

327. The IoM meets c.25.5, 25.6 and 25.7 and mostly meets c.25.8. It partly meets c.25.1 to 25.4. **R.25 is rated partially compliant**.

Recommendation 26 – Regulation and supervision of financial institutions

328. *Criterion 26.1* (Mostly met) - The IOMFSA is a single supervisory authority, which is charged with responsibility for the regulation and supervision of FIs under the FSA 2008 and DBRO Act. However, not all of the activities or operations listed in the FATF's definition of "financial institution" are regulated or supervised[94]. The effect of the scope gap is thought to be minor.

329. The IOMFSA's functions under Schedule 1 of the FSA 2008 include the regulation and supervision of persons undertaking "regulated activities"[95] [under the FSA 2008], "regulated insurance activities" [under the IA 2008] and "regulated pension activities" [under the IA 2008 and RBSA 2000] which it undertakes in line with its statutory objective to reduce financial crime.

[94] Schedule 4 of the POCA 2008 does not cover all elements of: (i) participation in securities issues and provision of financial services related to such issues; or (ii) investing, administering or managing funds or money on behalf of other persons.

[95] Sec. 3 of the FSA 2008 specifies that an activity is a "regulated activity" if it is a "financial services activity" of a specified kind and it is undertaken by way of business. The RAO 2011 specifies the "financial services activity" that is to be considered a "regulated activity" and encompasses: (i) deposit taking; (ii) investment business; (iii) provision of services to CIS (such as by managers and administrators); (iv) payment services (including money transmission services, bureaux de change, and e-money); and (v) trust and corporate services.

In addition, para. 2(1) (ba) of Schedule 1 recognises explicitly that a function of the IOMFSA is the "conduct of investigations into any potential liability arising from breach of AML/CFT legislation by persons undertaking regulated activities".

330. As a result of exclusions included in the RAO 2011, the IOMFSA does not have the power to supervise compliance by a number of persons carrying on activities that are subject to the AML/CFT Code, but which are not also subject to the FSA 2008. In all but one case[96], the effect of the RAO 2011 appears to be to exclude activities from supervision which the evaluation team does not consider to be those undertaken by a FI (as defined by the FATF).

331. As for FIs covered by the DBRO Act[97] since 26 October 2015, sec. 5 of the DBRO Act makes the IOMFSA responsible for assessing compliance with AML/CFT legislation, and where any breach of that legislation is found, conducting investigations into any potential criminal liability arising from that breach.

332. *Criterion 26.2* (Mostly met) - Persons carrying on "regulated activities" must hold a licence issued under sec. 7 of the FSA 2008, except where they are covered by a licensing exemption under the Financial Services (Exemptions) Regulations 2011[98]. Insurers are authorised under sec. 8 of the IA 2008 and administrators of retirement benefit schemes are registered under sec. 36 of the RBSA 2000. In addition, some collective investments schemes must be authorised under the CISA 2008. Other FIs are required to be registered under Sec. 7 of the DBRO Act.

333. The IOMFSA publishes a General Licensing Policy ("GLP") under sec. 6(3) of the FSA 2008 which sets out the criteria normally applied by the IOMFSA when considering the fitness and propriety of persons seeking a licence and those already licensed under the Act. Para. 2.8.1 of the GLP states 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. An applicant can demonstrate real presence by satisfying the FSC [now the IOMFSA] that the business' centre of activity will be in the IoM". Furthermore a physical presence is required under sec. 6 (1) (d) of the FSA 2008.

334. *Criterion 26.3* (Met) - According to sec. 6 of the FSA 2008, a licence will not be issued unless the IOMFSA is satisfied that the applicant, any "controller"[99] or director thereof, and any other person as appears to the IOMFSA to be a key person is "fit and proper". The IOMFSA also has powers under sec. 10 of the FSA 2008 to direct that a FI cannot appoint a director, controller or key person or continue in such a role.

335. The list of examples of matters the IOMFSA may have regard to in determining whether a FI or controller, shareholder, director or key person is fit and proper is set out in Appendix 3 to the GLP. The GLP goes on to state that the list is illustrative only and the IOMFSA will also consider any other relevant matter in addition, or alternatively, to the matters listed.

336. Similar provisions are set out in sec. 7 and 29 of the IA 2008 for insurance business, sec. 19 and 36 of the RBSA 2000 for retirement benefit scheme administrators and sec. 9 of the DBRO

---

[96] The FSA cannot supervise compliance with AML/CFT requirements by the manager of a single exempt scheme (a private collective investment scheme) that operates on a commercial basis.

[97] Schedule 1, Part 1, point 1 letters (f) to (h) cover: (i) the business of lending, having the meaning in para. 1(1)(ff) of Schedule 4 of POCA 2008; (ii) the business of financial leasing arrangements, having the meaning in para. 1(1)(gg) of Schedule 4 of POCA 2008; and (iii) the business of providing financial guarantees and commitments, having the meaning in para. 1(1)(hh) of Schedule 4 of POCA 2008.

[98] The authorities have not provided evaluators with an explanation of the basis for these exemptions from licencing – which include Core Principles financial institutions. They have explained that exemptions are varied in nature, are in use by regulators worldwide and tend to be used in areas where licensing would be disproportionate.

[99] According to sec. 48 of the FSA 2008, a controller is a person who either alone, or with any associate or associates, is entitled to exercise or control the exercise of 15% or more of the voting power at any general meeting of the licence holder or of another body corporate of which it is a subsidiary, so this term covers also beneficial owners.

Act for other FIs. In addition, the CISA 2008 specifies that each person comprising the governing body of a collective investment scheme must be fit and proper in line with the GLP. See CISA 2008, Schedule 1, para. 2(9) and (10), Schedule 2, para. 2(8) and (9), and Schedule 4, para. 2(6).

337. The DBRO Act specifies that the IOMFSA must refuse to register an applicant if it is not satisfied that the "applicant or a specified person in relation to the applicant" is a fit and proper person, and the perimeter of the testing is more limited than under the FSA 2008 and IA 2008. However, as the DBRO Act relates to FIs other than Core Principles FIs the safeguards in place may be deemed proper.

338. *Criterion 26.4* (Met) - All Core Principles FIs (plus money value transfer services, currency changing services, retirement benefit scheme administration and others) regulated under the FSA 2008, IA 2008 and RBSA 2000 are subject to regulation and risk-based supervision, where AML/CFT risk is taken into consideration.

339. A holistic approach to risk is set out in the IOMFSA's Supervisory Approach document, which applies to FIs regulated and supervised under the FSA 2008 and addresses prudential and conduct of business matters as well as ML/TF. It is, however, not binding upon the IOMFSA or FIs. The Supervisory Approach document applies indirectly to the oversight of collective investment schemes – through the supervision of functionaries of such schemes.

340. There is no specific equivalent of the Supervisory Approach document for life assurance companies or pension scheme administrators. However, risk assessments consider three broad categories of risk split into three parts: financial; business; and regulatory (including ML/TF). There is a less formalised approach (than life assurance) to risk assessments for the pensions sector. However, all available data is taken into account to make an informal on-going risk assessment.

341. The IOMFSA has just two licence holders (both banks) with branches outside the IoM (one in the UK and two in the Channel Islands) and two (one investment business and one payment services provider) with overseas subsidiaries (one in the UK and another in Mauritius). In the case of branches, input is sought annually from host regulators.

342. The DBRO Act came into force on 26 October 2015 and FIs within its scope have been subject to supervision since 1 January 2016. Compliance with national AML/CFT laws are reviewed during an on-site inspection.

343. *Criterion 26.5* (Mostly met) – All FIs are now subject to a risk-based approach to AML/CFT supervision (a number having been subject to supervision by the IOMFSA since October 2015). The AML/CFT risk is taken into account when determining the frequency and intensity of both on-site and off-site AML/CFT supervision.

344. In accordance with the Supervisory Approach, the risk profile of a FI (taking into account financial failure, misconduct, fraud and ML/TF) and the impact that its failure would have on the IOMFSA's consumer protection objectives drive the type of on-site visits carried out by the IOMFSA, the areas to be examined, and the frequency of on-site visits. However, the actual frequency and type of visits will depend not only upon the FI's overall rating, but also on the nature of the risks identified. The IOMFSA performs both on-site and desk-based supervision, the results of which are fed into the on-going risk assessment of the licence holder. The IOMFSA has explained that, in the case of a licence holder with: (i) low risk of failure; (ii) low risk of misconduct and fraud; and (iii) high risk of ML/TF, risk assessments would not be averaged. Instead, the institution would be considered to present a high risk (because of its ML/TF risk assessment) and ML/TF the focus of supervision on the basis of such a risk assessment. A similar approach is applied to life assurance companies and pension administrators.

345. For FIs supervised under the DBRO Act, the risk assessment is initially based on a desk-based analysis of the profile of the applicant's business, making use of a questionnaire which analyses

the size of the business, its markets, its customer demographics and procedures. The results of this assessment then determine how quickly a business will be subject to an on-site visit. Following this initial visit, findings will be used to form an on-going assessment which will dictate, on a risk-based approach, when the business will be visited next. The IOMFSA will be conducting an onsite evaluation of all FIs regulated under the DBRO Act within the first 3 years of the legislation's operation, after which designated businesses will be visited at least once every 6 years – dependent upon risk.

346. The IOMFSA has explained that planning of visits (by sector and across sectors) takes into account areas that it wishes to focus on, using its knowledge of where risks may be higher. At the time of the onsite visit, the basis for this risk assessment process had not yet been documented[100]. However, the IOMFSA has not clearly articulated how the frequency and intensity of supervision takes account of the degree of discretion given to FIs in application of the AML/CFT Code – in particular reliance on third parties and application of exemptions (with greater focus expected on these areas for those institutions or groups exercising discretion), though these areas are considered in themed visits.

347. *Criterion 26.6* (Met) - For FIs that are regulated under the FSA 2008, the Supervisory Approach notes that risk assessments are updated to reflect new information as it becomes available. Every risk assessment is updated at least annually to reflect the annual desk-based review. Visits and other material events also trigger updates of risk ratings. The risk assessment of each life assurance company is updated on a quarterly basis upon receipt of quarterly returns and on the occurrence of trigger events such as recent on/off site inspections (if applicable), press releases, complaints, etc. Risk assessments in respect of pension administrators are undertaken on an annual basis.

348. For FIs supervised under the DBRO Act, the authorities have explained that risks presented are reassessed following a visit, at the point of a material change in business (which must be notified to the IOMFSA under sec. 19 of the DBRO Act) or upon receipt of intelligence.

Weighting and Conclusion

349. The IoM meets c.26.3, 26.4 and 26.6 and mostly meets c.26.1, 26.2 and 26.5. **R.26 is rated largely compliant**.

Recommendation 27 – Powers of supervisors

350. *Criterion 27.1* (Mostly met) - As explained under c.26.1, the IOMFSA has responsibility for supervising and ensuring compliance by nearly all FIs (term as defined by the FATF) with AML/CFT requirements. Its powers derive from this responsibility. The effect of the scope gap identified at c.26.1 is thought to be minor.

351. *Criterion 27.2* (Met) - In line with sec. 15 and Schedule 2 of the FSA 2008, the IOMFSA may inspect the books, accounts and documents, and investigate the transactions of a "permitted person" (a person holding a licence under the Act); a former permitted person; or a recognised auditor (but only insofar as concerns the audit of "market traded" companies). The provision also gives powers of entry and access, and taking possession of all such books, accounts and documents as, and for so long as, may be necessary for supervisory purposes. Similar provisions are in place under sec. 36 and Schedule 5 of the IA 2008 in respect of insurance and pension entities, and under sec. 14 of the DBRO Act in relation to FIs supervised under that Act. Failure to permit inspection is an offence.

[100] Since the on-site visit, the IOMFSA has started to produced overview documents for each sector which provides a sector overview, identifies trends, macro developments, risks and threats (in order of priority), identifies supervisory risks, and considers resourcing, supervisory tools, and characteristics of FIs and groups (including diversity and number). Documents address ML/TF risk. The IOMFSA has explained that these overview documents will be presented to the Board.

352. *Criterion 27.3* (Mostly met) - Under para. 2(1) of Schedule 2 of the FSA 2008, the IOMFSA may request any person whom it reasonably believes may hold information that it reasonably requires for the performance of its functions to provide that information. According to para. 2(3) if the request was made of a permitted person, former permitted person, recognised auditor or former recognised auditor, the IOMFSA may issue directions to that person to secure that effect is given to its request. If a person contravenes any direction by the IOMFSA, the Authority may undertake action for a breach. The IOMFSA is also able to compel production of information from any other person whom it has reason to believe holds relevant information when it is authorised to do so by a justice of the peace (magistrate) under para. 3. Similar powers are vested with the IOMFSA in para. 2 of Schedule 5 to the IA 2008 and sec. 15 of the DBRO Act except that, in both cases, the IOMFSA may direct any person whom it has reason to believe holds relevant information to secure that effect is given to a request. Failure to provide information is an offence.

353. Under sec. 13 of the CISA 2008, the IOMFSA may appoint a person to advise a collective investment scheme on the proper conduct of its affairs or appoint a person to assume control of the affairs of the scheme. This is in addition to the IOMFSA's powers over the functionaries of such schemes (permitted persons) which allow it to require the functionary to provide information about its customers (i.e. schemes).

354. *Criterion 27.4* (Met) - The IOMFSA is authorised to impose sanctions for failing to comply with AML/CFT requirements under the FSA 2008, IA 2008, RBSA 2000, CISA 2008 and DBRO Act 2015. These include powers to withdraw, restrict or suspend a FI's licence, to impose a fine, and to prohibit people who are not fit and proper from discharging their functions. The regulator's powers are considered further at c.35.1.

Weighting and Conclusion

355. The IoM meets c.27.2 and 27.4, and mostly meets c.27.1 and 27.3. **R.27 is rated largely compliant**.

Recommendation 28 – Regulation and supervision of DNFBPs

356. *Criterion 28.1* (Mostly met) - Casinos (including online gambling)

357. The supervisory body for gambling activities is the GSC, with the following regulatory objectives (sec. 5 of the GSA 2010): (i) ensuring that gambling is conducted in a fair and open way; (ii) protecting children and other vulnerable persons from being harmed or exploited by gambling; and (iii) preventing gambling from being a source of crime or disorder, associated with crime or disorder, or used to support crime.

358. Casinos operators in the IoM (currently just one), as well as online gambling operators, have to hold a licence granted by the GSC (sec. 1A of the CA 1986 and sec. 4(1) of the OGRA 2001 respectively).

359. In the case of a casino, the decision to grant a licence rests not with the GSC but with the IoM's Council of Ministers. According to sec. 3(6) of the CA 1986, the Council of Ministers shall not grant a casino licence to any person unless it is satisfied (amongst other matters) that he is a person of integrity; and, in the case of a licence intended to be granted to a body corporate, that the relevant share capital of the body is beneficially owned by a person or persons of integrity. Fit and proper testing extends to directors of a licence holder (sec. 4) and persons employed or engaged by the licence holder to perform any function stated in sec. 17 of CR 2011. In order to form a view on integrity, any criminal convictions highlighted by background checks on the applicant, its owners, controllers and key staff, and personal references will be taken into account. In practice, these fit and proper tests are delegated to the GSC.

360. For online gambling, the GSC's Commissioners shall not grant a licence to any company under sec. 4(2) of the OGRA 2001, unless they are satisfied (inter alia): (i) that the company is under

the control of a person or persons of integrity; (ii) as to the beneficial ownership of the share capital of the company; and (iii) that the activities of the company are under the management of a person or persons of integrity and competence. Each of these controllers or managers is required to complete a personal declaration form, part 2 of which requires, e.g. disclosure of criminal convictions, and cautions and warnings received.

361. Sec. 10 of the OGRA also prohibits the GSC from approving a designated official (director of the licence holder) unless satisfied as to the individual's integrity and competence. However, these provisions do not clearly extend to "operators" (which may be different to licence holders and who may not also be owners, controllers or hold a management function).

362. Whereas sec. 5 of the CR 2011 empowers the GSC to carry out inspections of any casino for the purpose of ensuring that the CA 1986 and Regulations are observed, there is currently no direct provision in law to empower the GSC to conduct AML/CFT oversight. Instead, a condition has been added to the sole casino's licence (with effect from 1 February 2016) in order to provide a clearer statutory basis for oversight. Notwithstanding the absence of such a condition, the GSC has, in fact, overseen compliance for many years.

363. Similarly, sec. 11 of the OGRA 2001 provides the GSC with responsibility for supervising the operation of online gambling conducted in the IoM with a view to securing that it is fairly and properly conducted and that the provisions of the Act and regulations, and the conditions of licences, are complied with. Whilst these powers do not directly relate to AML/CFT matters, the conduct of an online gambling operator includes adherence to AML/CFT requirements through licencing conditions[101]. Sec. 16 of the OGRA 2001 provides the GSC with the necessary powers to exercise any function at any time to: (i) enter any premises where there is reasonable cause to believe they are or have been used for any purpose connected with the conduct of online gambling; (ii) require any person to produce any documents or other records relating to, or connected with, the conduct of online gambling, and to take copies of such documents or records; and (iii) require any person to provide access to any computer program used, or to be used, in connection with the conduct of online gambling. Sec. 16(4) of the OGRA 2001 also make it an offence for an online gambling operator to intentionally obstruct another in the exercise of a power, the effect of which is to require a person to answer questions set by the GSC.

364. *Criterion 28.2* (Mostly met) - DNFBPs other than casinos

365. The IOMFSA is the designated authority to monitor and ensure compliance of DNFBPs (except gambling) with AML/CFT requirements. TCSPs are regulated and supervised under the FSA 2008 in line with other "regulated activities" and other DNFBPs (as defined by the FATF) are supervised for AML/CFT purposes under the DBRO Act 2015. However, it is noted that acting as a partner is not regulated or supervised under Class 4 of the FSA 2008[102].

366. As a result of exclusions included in the RAO 2011, the IOMFSA does not have the power to supervise compliance by a number of persons carrying on TCSP activities subject to the AML/CFT Code, but which are not also subject to the FSA 2008. The effect of the RAO 2011 appears to be to exclude activities from supervision which the evaluation team does not consider to be those undertaken by a TCSP (as defined by the FATF).

367. *Criterion 28.3*. (Met) - DNFBPs other than casinos

[101] All OGRA licences include the same wording re AML/CFT: "The licensee must fully comply with any AML/CFT provisions that apply to the business and/or any type of gambling permitted under Schedule 1 of this licence."

[102] In practice, it is noted that a person acting as partner to a partnership is likely also to be providing other TCSP services and so the gap identified is not likely to be significant.

368. All categories of DNFBPs (except gambling) regulated in the IoM are subject to on-site and off-site supervision by the IOMFSA in accordance with the FSA 2008 and DBRO Act. In the case of DNFBPs supervised under the DBRO Act, this commenced on 1 January 2016.

369. The IOMFSA has a power to delegate its oversight powers under the DBRO Act to third parties and has delegated its powers to the: (i) ICAEW; (ii) ACCA; (iii) IoM Law Society; (iv) International Association of Bookkeepers; and (v) Institute of Certified Bookkeepers. These bodies undertake visits of their own members in place of the IOMFSA, but are required to follow IOMFSA guidelines and procedures so that visits are conducted in a consistent manner.

370. *Criterion 28.4.* (Met) -DNFBPs other than casinos

371. The IOMFSA's powers under the FSA 2008, described under R.26 and R.27, are applicable to TCSPs. DNFBP specific on-site and off-site supervisory powers, as well as fit and proper testing and sanctioning powers, are set out in the DBRO Act and are also described under R.26 and R. 27.

372. Where an activity is listed in the Financial Services (Exemptions) Regulations 2011, the effect is to exclude that activity from up front measures to prevent criminal involvement. One such exemption covers an individual who is not, and does not act as, a director of more than 10 companies. A similar exemption applies to lawyers and accountants that do not hold more than 10 appointments as either a trustee or protector of a trust or as an enforcer of a trust or foundation. A person subject to such exemptions is still covered by all of the other powers and sanctions available to the IOMFSA, which could be used to prevent criminal involvement.

373. Separately, the Law Society and UK professional accounting bodies also take measures to prevent criminals from becoming members of their respective bodies.

374. All Manx advocates, regardless of previous qualifications in another jurisdiction, have to: (i) undergo police and regulatory checks; (ii) pass an interview with the Council of the Society; (iii) be approved by the First Deemster (judge); (iv) enter a period of training under an established senior advocate; (v) attend a further interview with the Council of the Society; (vi) make a written declaration regarding AML/CFT compliance and bankruptcy etc.; and (vii) receive final approval to enter the Manx Bar from the First Deemster.

375. The ICAEW requires confirmation that an individual is "fit and proper" at three points before they can become an ICAEW member: (i) when they apply to be a student (self-declaration); (ii) when they submit their training record of eligibility (also signed by their qualified partner responsible for training); and (iii) when they apply for their membership – which should again be endorsed by their training office. If a member wants to practice as an accountant, they must comply with the ICAEW's continuing professional development requirements, its Code of Ethics, hold professional indemnity insurance and be "fit and proper".

376. Sanctions are available to the IOMFSA under the FSA 2008 and DBRO Act to deal with failure to comply with AML/CFT requirements. These are explained under c.35.1. These include powers to withdraw, restrict or suspend a DNFBP's licence, to impose a fine, and to prohibit people who are not fit and proper from discharging their functions. The regulator's powers are considered further at c.35.1.

377. *Criterion 28.5* (Mostly met) - All DNFBPs

378. The application of a risk-based approach to TCSPs under the FSA 2008 (Supervisory Approach) and other DNFBPs under the DBRO Act is explained under R.26.

379. The IOMFSA has not clearly articulated how the frequency and intensity of supervision takes account of the degree of discretion given to DNFBPs in application of the AML/CFT Code – in particular reliance on third parties and application of exemptions (with greater focus expected on these areas for those institutions or groups exercising discretion).

380. Historically, the GSC has not applied a risk-based approach to online gambling operators and has instead inspected all licensees whether large or small as part of a rolling programme. Post NRA, it has conducted informal AML/CFT focused visits of all online gambling operators with the primary aim of checking and reinforcing its assessment of the sector. Over 30 formal follow-up visits have subsequently taken place and the findings from these formal visits will assist the GSC in risk assessing each of its licence-holders so that it can move to a risk-based approach to AML/CFT supervision in 2016 and onwards. Online gambling operators are assessed for compliance in ten areas: risk-based approach; CDD; PEP and sanctions screening; enhanced CDD; on-going monitoring; record-keeping; role of ML reporting officer; suspicious activity reporting; staff vetting and training; and compliance culture.

381. There is just one casino which is visited each month.

Weighting and conclusion

382. The IoM meets c.28.3 and 28.4 and mostly meets c.28.1, 28.2, and 28.5. **R.28 is rated largely compliant**.

Recommendation 29 - Financial intelligence units

383. In its 2009 Report, the IoM was rated largely compliant with these requirements (paras. 291 to 331). The deficiencies related to the absence of a formal power of access to additional information for analytical purposes and limited effectiveness of the overall reporting system, as was reflected in low numbers of domestic FCU investigations. Since the 2009 Report, the FATF Standards have been significantly strengthened in this area, and more importantly, the IoM's FIU has changed its legal structure.

384. *Criterion 29.1* (Met) - As a result of the FIU Act enacted in April 2016, the FIU was established as a stand-alone body corporate. The FIU is constituted to serve as the national centre for receipt, analysis and dissemination of all relevant ML and TF information: sec. 5(1) and (2) of the FIU Act 2016.

385. *Criterion 29.2* (Met) - The FIU serves as the central agency for the receipt of disclosures filed by reporting entities, including: (i) SARs; and (ii) declarations on cross-border currency and BNIs. Declarations on cross-border transportation of currency and BNIs are automatically forwarded to the FIU by the CED.

386. *Criterion 29.3* (Met) - The FIU may request from reporting entities any information and documentation needed to perform its functions: FIU Act 2016, Part 4, sec. 18. This includes additional information from reporting entities which had not originally submitted a SAR. The FIU, as a joint police/customs unit, has full and direct access to an extensive range of administrative, law enforcement, and financial information apart from its own database. The FIU can also access many UK law enforcement databases.

387. *Criterion 29.4* (Mostly met) - The FIU undertakes operational analysis based on the information received from reporting entities and other information available to it. The FIU utilises the IoM Constabulary's IT system for its information management regarding SARs and uses other in-house IT systems, including analytical tools. There is no requirement in law for the FIU to undertake strategic analysis and the analysis mainly comprises checking databases, making further enquiries, and comparison with ML/TF typologies. Nevertheless, the FIU conducts some degree of strategic analysis on ML/TF typologies and trends which are shared with industry.

388. *Criterion 29.5* (Met) - The FIU is authorised to disseminate (spontaneously or upon request) the results of its operational analysis to competent judicial bodies, law enforcement and regulatory authorities. FIU information can also be supplied to foreign law enforcement and prosecution authorities: POCA 2008, Part 6, sec. 210 to 214 and ATCA sec. 56 and 57. The FIU uses dedicated, secure and protected channels for the dissemination.

389. *Criterion 29.6* (Met) - The FIU protects its information through a number of rules and regulations in place governing the security and confidentiality of information[103]. All FIU information is registered and stored in the Government/Police secure computer server and can only be accessed by authorised personnel. Part 5 of the FIU Act 2016, sec. 26, creates an offence for failing to comply with a restriction in respect of further dissemination of information supplied by the FIU. All personnel are subject to vetting checks on employment and are subject to security clearance to a 'secret' level and are also subject to the OSA 1989 as well as legislative requirements regarding confidentiality. Access to the FIU's facilities and information, including IT systems, is restricted and protected. FIU-specific information, such as SARs and information from foreign FIUs, is stored on the secure police computer. Physical access to the FIU is restricted to special entry pass holders.

390. *Criterion 29.7* (Met) - The FIU is a stand-alone body corporate, operationally independent of both the IoM Constabulary and the CED, with its own secure premises. While being subordinated to the DHA and guided by the FIU Board, the FIU has operational autonomy and independence: Sec. 5, 6 and 8 of the FIU Act 2016. The Director of the FIU is appointed by the DHA in consultation with the FIU Board which also oversees the FIU by approving its general operational policy, guidelines, directions and strategic priorities. These guidelines are general in nature and do not refer to operational matters such as specific SARs or other sources of information which are to be disseminated by the FIU on a strictly technical basis. Such operational decisions are left to the FIU's discretion.

391. The FIU is able to make arrangements or engage independently with other domestic competent authorities or foreign counterparts on the exchange of information: POCA 2008, Part 6, sec. 210 to 214; the FIU Act 2016, sec. 7. The FIU does not need permission to undertake dissemination of information or sign memoranda of understanding, either domestically or internationally. The FIU appears to be free from political or industry control, interference or undue influence, with its own separate budget, and no ministers or otherwise elected members of the Government sitting on the Board of the FIU.

392. *Criterion 29.8* (Met) - The FIU has been an active member of the Egmont Group since 2000.

Weighting and conclusion

393. The IoM meets all criteria except for c.29.4, which is mostly met. **R.29 is rated largely compliant**.

Recommendation 30 – Responsibilities of law enforcement and investigative authorities

394. In its 2009 Report, the IoM was rated largely compliant with these requirements. The deficiency noted related to effectiveness which is not assessed as part of technical compliance under the 2013 Methodology.

395. *Criterion 30.1* (Met) - The investigative branch of the FCU is responsible for the investigation of ML and TF. It is a joint police and customs department. The CED is empowered to administer, investigate and enforce the various provisions of customs and excise legislation as well as other legislation with regard to so-called "assigned matters". Assigned matters include drug trafficking and ML related to customs offences (such as indirect tax, VAT fraud and smuggling), and enforcement of UN and EU sanctions, particularly in relation to terrorism assets (sec. 184(1) of the Customs and Excise Management Act 1986). There are specialised departments within the IoM Constabulary responsible for several of the categories of predicate offences, including drug

[103] The IoM Government Corporate Information and Records Management Policy, 2011 which conform with the principles of ISO 15489; Police Disciplinary Regulations 2015 for Police Officers; the IoM Civil Service Regulations for customs officers and civil servants - for disciplinary matters; and the Official Secrets Act protecting the confidentiality of the information.

trafficking. This responsibility, however, is at an operational level and is not mandated in law. The Attorney General's Chambers (AGC) provides legal advice and expert assistance in all investigations, including ML and TF.

396. Criterion 30.2 (Met) - There is no explicit requirement in POCA 2008, PPPA 1998 or in the customs law for a parallel financial investigation to be undertaken. The authorities stated that, in practice, a joint agency approach is taken to any criminal investigation in order to utilise the expertise of the FCU in such investigations. The FCU will, at the same time, also be responsible for the required parallel financial investigation and any related ML offences.

397. *Criterion 30.3* (Met) - The IoM Constabulary is empowered to identify, trace, seize and initiate freezing and seizing of property that is, or may become, subject to confiscation, or is suspected of being the proceeds of crime. The powers are set out in the sec. 26 of the PPPA, and Schedule 1A. The POCA 2008 (s.169(4)) confers specific powers on police officers. The police may also act under court orders (s.26 J (10) (B) PPPA 1998 – right to apply to a judge for return of seized items).

398. *Criterion 30.4* (Met) - As mentioned above, the FCU is in charge of conducting financial investigations in the IoM. The CED is empowered to administer, investigate and enforce the various provisions of customs and excise legislation as well as other legislation with regard to so-called "assigned matters" as described under c. 30.1 above. Other relevant bodies (such as the financial supervisors and the Assessor of Income Tax) must collaborate in the fight against ML/TF by exchanging information with the FCU. The exchange of information for the purposes of combating and preventing ML/TF between the FCU, supervisory authorities, and other competent authorities usually takes the form of a joint agency approach, as described under c.30.2 above.

399. *Criterion 30.5* (Not applicable) - There are no specialised units dealing with corruption offences in the IoM. The criterion is therefore not applicable.

Weighting and conclusion

400. The IoM meets all the applicable criteria under R.30. **R.30 is rated compliant**.

Recommendation 31 - Powers of law enforcement and investigative authorities

401. In the 2009 Report, the IoM was rated compliant with R. 28.

402. *Criterion 31.1* (Met) - The competent authorities conducting investigations of ML/TF and associated predicate offences can obtain access to all necessary documents and information for use in those investigations, prosecutions, and related actions through various provisions under the POCA 2008[104], PPPA 1998 (sec. 11 to 26, and 57 and 58), ATCA (sec. 18, 24, 25, 31, 32 and Schedules 4, 5, and 6). The AGC has special powers to obtain evidence without a court order in respect of serious or complex fraud, wherever committed (the CJA 1991 sec. 24 and the CJA 1990 sec. 25). The AGC has the power to require the production of evidence and it is an offence to refuse to comply. The powers outlined above are also available to Customs Officers who are included within the definition of 'Constables' within the Acts. All law enforcement officers are entitled and have the power to take witness statements.

403. *Criterion 31.2* (Met) - The competent authorities are able to use a wide range of investigative techniques for investigating ML/TF and associated predicate offences, including undercover operations, intercepting communications, accessing computer systems, and controlled delivery. Although there is no formal statutory requirement in the IoM for an undercover operation to be authorised, there is authority at common law that undercover operations should be so authorised. The authorities claim that undercover operations have been successfully completed by the IoM Constabulary, leading to prosecutions and convictions on the IoM, which is supported

[104] Sec. 43, 162, 169-173, 174-179, 180-192.

by at least one case provided by the authorities.[105] The issues of intercepting communications, accessing computer systems and controlled delivery are covered by the relevant provisions in the Interception of Communications Act 1988, s.23 of the PPPA 1996, s.166 and 169 of POCA 2008, sec. 166A and Part VA of the Customs and Excise Management Act 1986, and sec. 15 and 49 of the Post Office Act 1993.

404. *Criterion 31.3* (Met) - Part 4 of POCA and sec. 18, 24, 25, 31, 32 and Schedules 4, 5 and 6 of ATCA provide for account monitoring orders, customer information orders, disclosure orders, search warrants and financial information orders, issued by the appropriate court at the application of a constable. These powers allow investigators to identify, in a timely manner, whether natural or legal persons hold or control accounts or identify assets, without prior notification to the owner.

405. *Criterion 31.4* (Met) - The competent authorities investigating ML, TF and associated predicate offences are able to ask for all relevant information held by the FIU, and may use such information as intelligence to further their investigations. The FIU is legally responsible for providing assistance to the Attorney General, Chief Constable, any law enforcement agency and the competent administrative bodies: sec. 6 of the FIU Act 2016.

Weighting and conclusion

406. The IoM meets all the criteria. **R.31 is rated compliant**.

Recommendation 32 – Cash Couriers

407. In the 2009 Report, the evaluators found that the cross-border control regime at the time did not cover cash transportation by mail between the UK and the IoM. As a result, the recommendation was rated largely compliant. In 2013, the law was amended to rectify the deficiency. Other amendments were carried out to further strengthen the system.

408. *Criterion 32.1 and 32.2* (Met) - The IoM applies a declaration system. A person entering or leaving the IoM and carrying, or otherwise having in their possession or control, cash with a value in excess of EUR 10 000 must declare that value to a customs officer (sec. 76C(1) of CEMA). The requirement applies to movement of cash from or to the Common Travel Area (the UK, Ireland, the Channel Islands and the IoM) and any other place: Part VA of CEMA, sec. 76B (exporting or importing goods), 76CA (sending or receiving postal packets) and 76E (cash on ships and aircraft or in goods). Cash includes notes and coins in any currency and BNIs as defined in the FATF Glossary (sec. 76A(1) of CEMA). Since June 2015, it also includes stored value cards and other documents, devices, coins or tokens with a monetary value.

409. Information on the cash declaration system is provided on the CED pages of the Government website and within a public notice on the CED front page (An introduction to cash entering or leaving the IoM). A further public notice (Notice 9011) and the form (Form C9011 MAN) for making the declaration are also available on the website. The form requires the declarant to provide prescribed details.

410. The requirement applies to cash sent in the mail (including mail moving to and from the UK, which is otherwise treated as domestic) or sent or carried in cargo, by courier fast parcel service, or in any other way: sec. 76B (exporting or importing goods), 76CA (sending or receiving postal packets) and 76E (cash on ships and aircraft or in goods) of CEMA.

411. *Criterion 32.3* (Not applicable)

412. *Criterion 32.4* (Met) - Customs officers may ask questions about the origin of cash and its intended use and questions designed to find out if the cash is property obtained through unlawful conduct or is intended to be used for ML or other unlawful conduct or activities related

[105] The case of Trevor Anthony Cooil (Crim 2000/29) which concerned an undercover drugs operation.

to terrorism (sec. 76F of CEMA). Questions may be asked by a customs officer not only upon the discovery of a false declaration or a failure to declare but also whenever a person makes a truthful declaration. The officer may also require evidence in support of any information to be provided.

413. *Criterion 32.5* (Met) - Persons who make a false declaration or fail to submit a declaration are liable to a custodial penalty of up to 2 years, or a fine, or both. The authorities have stated that in serious cases, the provisions of the POCA 2008 (or even ATCA) could be applied, with charges of ML and/or confiscation or forfeiture of the cash involved.

414. *Criterion 32.6* (Partly met) - All declarations received by CED were previously routed to the FCU. Although the FIU established under the new FIU Act 2016 continues to receive cash declarations, as a separate organisation in its own right, it will require an order extending sec. 174B to it, and it is probable that a MOU will have to be agreed to formalise existing arrangements.

415. *Criterion 32.7* (Met) - Coordination between customs and other related authorities is mainly conducted through the Serious Crime Supervisory Board, involving the IoM Constabulary, the CED and the AGC and through the Joint Tasking Group, involving the IoM Constabulary, the CED, the FIU and the ITD. Both of these bodies meet on a regular basis. On the operational level, it appears that coordination between the CED and the immigration authorities is mostly done on an informal basis. There is also a 24-hour on-call immigration officer, to whom any serious or complex matters would be referred.

416. *Criterion 32.8* (Met) - Customs officers may seize cash, whether or not in excess of EUR 10, 000, where: (i) a person refuses to make a declaration or disclosure to an officer; (ii) an officer reasonably believes that a declaration or disclosure is untrue in a material particular; (iii) an officer has required further evidence in support of information provided in respect of a cash movement, and this has not been provided, or does not support the information; or (iv) the officer reasonably believes that any cash is property obtained by unlawful conduct, or is intended for use in ML, other unlawful conduct, or activities related to terrorism. (Sec. 76G of the CEMA, sec. 46 to 54 of POCA). The seized cash may be detained for as long as the reasonable suspicion remains or for an initial period of 48 hours.

417. *Criterion 32.9* (Partly met) - The CED may exchange any information in its possession with foreign authorities pursuant to sec. 174B of CEMA. There is no provision in CEMA requiring the CED to maintain records on: (i) declarations; (ii) false declarations; or (iii) ML/TF suspicions. However, declarations received by the CED are passed to, collated by, and maintained within the FCU, although without a legal provision in CEMA to do so (given the new FIU Act 2016, as noted under c.32.6). Also, sec. 174B of CEMA provides for the disclosure of information and documents to the Chief Constable and members of the IoM Constabulary.

418. *Criterion 32.10* (Met) - Information may only be disclosed in the cases referred to in sec. 174B of CEMA (see c.32.9). Additionally, disclosures may not be made if they are prohibited by any provision of the Data Protection Act 2002. These conditions do not restrict trade payments between countries for goods and services or the freedom of capital movements, in any way.

419. *Criterion 32.11* (Met) - In addition to those penalties contained in Part VA of CEMA set out under c.32.5 above, the provisions of Part 4 (ML) of POCA 2008 or sec. 10 (ML) of ATCA would also apply. These provide for a custodial sentence not exceeding 14 years or a fine, or both - on conviction. Cash which is seized under sec. 76G of SEMA includes cash being imported or exported, which the customs officer reasonably suspects is property obtained through unlawful conduct, or is intended to be used for ML or other unlawful conduct of activities or related to terrorism. This includes cash which does not exceed the declaration threshold (currently EUR 10 000) where such suspicions arise. Once seized under sec. 76G, sec. 47 to 54 of the POCA 2008 apply. Sec. 50 of POCA 2008 provides for the High Bailiff to order forfeiture of detained cash (or

any part of it) if satisfied that the cash (or the part of it) is recoverable property or in intended for use by any person in unlawful conduct (conduct which is unlawful under the criminal law of the IoM or unlawful under the criminal law of another country and which would be unlawful if it occurred in the IoM).

Weighting and Conclusion

420. The IoM meets all criteria except c.32.6 and c.32.9 which are partly met. There is no formal legal arrangement between the CED and the FIU that would allow the FIU to receive disclosures on cross-border transportation of currency and BNIs. **R.32 is rated largely compliant**.

Recommendation 33 – Statistics

421. In its 2009 Report, the IoM was rated largely compliant with these requirements. The main technical deficiency was that the IoM did not maintain comprehensive statistics on seizures and confiscations. While the language of R.33 has not changed, the Recommendation has become more relevant in the context of assessing effectiveness.

422. *Criterion 33.1* (Mostly met) - Statistics on matters relevant to the effectiveness and efficiency of the AML/CFT system in the IoM are maintained by various bodies.

423. STRs received and disseminated – The FIU records the total number of SARs received and disseminated, with further detailed breakdowns.

424. ML/TF investigations, prosecutions and convictions – The FCU maintains statistics in relation to ML/TF investigations (cases) carried out independently without a prior SAR, including the number of persons charged, prosecutions commenced and first instance and final convictions. It appears that the FCU had no readily available statistics on ML/TF investigations resulting from a SAR up until recently and a new core IT system is intended to be implemented to capture and collate statistics from different areas.

425. Property frozen; seized and confiscated – Statistics on frozen, seized and confiscated property is held by the Prosecution Division of the AGC. The NRA, however, recognises existing difficulties in collecting proper statistics on bulk cash smuggling cases and detected amounts as well as the absence of historical records of detected amounts.

426. MLA or other international requests for cooperation made and received - Statistics are maintained by the AGC in relation to MLA requests made and received. Records include the date the request is made and received, the unique reference allocated to it, the requesting country, the name of the person or entity and type of offence involved. The NRA, however, acknowledges that there is a need for such statistics to be kept centrally and updated regularly so that numbers received/responded to and the effectiveness of the IoM's response (including the timeframe) can be monitored at a national level.

Weighting and Conclusion

427. Although basic statistics are kept by the relevant competent authorities, there are gaps in the collection and maintenance of comprehensive statistics on matters relevant to the effectiveness and efficiency of the AML/CFT system, as demonstrated by the NRA. **R.33 is rated largely compliant**.

Recommendation 34 – Guidance and feedback

428. *Criterion 34.1* (Mostly met) - In respect of FIs and DNFBPs supervised under the FSA 2008 and DBRO Act, the IOMFSA has published an AML/CFT Handbook (guidance) which is designed to supplement the AML/CFT Code and to assist compliance with AML/CFT legislation. The main body of the Handbook was substantially changed in April 2015 to take account of the revised AML/CFT Code, which came into force in at that time. Sec. in the Handbook – which are generic to allow them to be used by a broad range of businesses - cover, amongst other matters: risk

assessments and on-going monitoring; CDD; simplified CDD; unusual activity and suspicious activity (including detecting, investigating and reporting); and compliance. The sec. on detecting, investigating and reporting was written with the assistance of the FIU. Where guidance is followed, the AML/CFT Handbook explains that this will tend to indicate compliance with legislative provisions.

429. Sector specific guidance (within the AML/CFT Handbook) was also published in April 2015 and has been developed in conjunction with relevant professional bodies. It covers the following areas: banking; TCSPs; funds and investment business (covering the securities sector); money transmission services; payroll agents; accountants and tax advisors; advocates and registered legal practitioners; estate agents; money lenders; specified non-profit organisations; high value goods dealers; and the IoM Post Office. Sector specific guidance in respect of virtual currency business is at an advanced stage of drafting. It had not been published at the time of the on-site visit.

430. Guidance Notes have also been published for the purpose of providing "binding guidance" for insurers undertaking long-term business. These came into force in September 2008 and so may not reflect current statutory requirements. They do not also cover insurance managers.

431. Online gambling service providers are required to comply with the provisions of the Online Gambling Code. Supporting guidance notes (guidance for AML-CFT online) were revised in December 2015 and are designed to clarify those areas in the Code that may be subject to varying interpretation; they also explain what the GSC is likely to expect as it conducts its regime of checking licence-holders' compliance with the Online Gambling Code.

432. The AML/CFT Handbook published by the IOMFSA has yet to be updated to take account of the NRA. The authorities have explained that the Handbook is likely to be updated in 2016. As noted above, the GSC has already updated its online guidance following the NRA and has discussed relevant NRA findings with online gambling operators on a one-to-one basis.

433. The IOMFSA has explained that there are a number of ways through which it provides feedback in relation to AML/CFT matters, including good and bad practice observed whilst onsite. In particular: (i) visit reports include action points that must be completed and best practice suggestions where applicable; (ii) conferences are organised by the IOMFSA, including its annual AML/CFT conference (last held in April 2015), and local professional bodies and trade associations; (iii) focussed outreach sessions; (iv) quarterly meetings are held with representative bodies of various sectors; (v) findings of thematic reviews (banking and insurance) are published; (vi) use is made of the IOMFSA's website to highlight enforcement action that has been taken; and (vii) guidance in the AML/CFT Handbook is updated. The supervisor also publishes an annual report which summarises work undertaken during the particular year under review.

434. The FCU provides aggregated feedback on reporting in the Chief Constable's Annual Report. It also has a page on the government website which provides information on reporting requirements and includes reporting forms to be used. It regularly takes part in educational seminars (averaging around 50 per annum according to the authorities) where it provides feedback on suspicious reporting. Advisory Notices are also circulated through the IOMFSA to MLROs covering topics such as IoM drugs trafficking typologies and operational cases. It has been explained that the FIU also periodically meets with IoM regulators to discuss SARs received and emerging trends, e.g. in the margins of AML/CFT Strategic Group meetings. For example, the FIU has met with the GSC on four occasions since 2012 to discuss the quality and timing of SARs, trends, chip-dumping and "consent process". However, the FIU does not routinely publish typologies drawn from its analysis of STRs.

435. The Law Society produces an annual summary of findings from its on-site visit programme. This highlights findings and themes which inform its oversight programme in the forthcoming

year, and provides support and guidance to members. The authorities have highlighted guidance and feedback provided by the ICAEW to its members in the Isle of Man and elsewhere. Whilst largely UK-focused, the more general elements of this guidance will assist accountants to meet AML/CFT requirements in the IoM.

436. No evidence has been provided of guidance and feedback provided by other competent authorities during the period under review.

Weighting and Conclusion

437. The IoM mostly meets criterion 34.1. **R.34 is rated largely compliant**.

Recommendation 35 – Sanctions

438. *Criterion 35.1* (Partly met)

Financial institutions and DNFBPs (except online gambling and casinos)

439. There is a broad range of sanctions (administrative, civil and criminal) available to deal with both natural and legal persons that fail to comply with the AML/CFT requirements. As noted under R.26, not all of the activities or operations listed in the FATF's definition of "financial institution" are regulated or supervised, and, consequently, the related sanctions do not apply to them.

440. The IOMFSA is vested by the FSA 2008 with administrative sanctioning powers which include the power to withdraw, restrict of suspend a FI's licence. In particular: (i) sec. 8 allows it to place conditions on a licence; (ii) sec. 9 allows it to revoke a licence; (iii) sec. 10 allows it to direct that an individual is unfit to be appointed, or continue as a director, controller or key person; (iv) sec. 10A allows it to prohibit people who are not fit and proper from discharging their functions; (v) sec. 13 gives it a power to issue a public statement; (vi) sec. 14 allows it to issue written directions, which may e.g. require the person to whom they are given to take such action in respect of any regulated activity as is specified in the direction; and (vii) sec. 16 specifies that the IOMFSA may impose a fine if it is satisfied that a FI has contravened any prohibition or requirement imposed under FSA 2008[106]. The level of that fine is established through the Financial Services (Civil Penalties) Regulations 2015 and based on a percentage of relevant income[107]. Unlike for the IA 2008, there is no provision to apply a penalty also to a controller, director, chief executive or senior manager of the licence holder.

441. FIs licenced under the FSA 2008 are also required to follow the FSRB. Where a person fails to comply with the FSRB, sec. 19(1) of the FSA 2008 states that the IOMFSA may take any of the actions listed under sec. 48(3) which is broadly drafted.

442. The IA 2008 also provides the IOMFSA with a range of administrative sanctions. In particular: (i) sec. 9 allows the IOMFSA to place conditions on an authorisation; (ii) sec. 10 allows the IOMFSA to withdraw a licence, but only to the extent that the authorised insurer concerned shall cease to be authorised to effect new contracts of insurance; (iii) sec. 29 allows the IOMFSA to prohibit people who are not fit and proper from discharging their functions; (iv) sec. 35 allows the IOMFSA to make a public statement; and (v) sec. 37 allows the IOMFSA to apply civil penalties where a person has acted in contravention of a requirement imposed by order under the Act[108]. Where the IOMFSA believes that a contravention of a requirement imposed by or under the IA 2008 was caused or permitted by a controller, director, chief executive or senior

[106] Sec. 19 of the FSA 2008 requires a licence holder to comply with the FSRB. Rule 8.5 of the FSRB mandates compliance with the AML/CFT Code.

[107] There are two levels of fine: level 1 – up to 5% of relevant income; and Level 2 – up to 8% of relevant income. These Regulations came into operation on 1 August 2015.

[108] Para. 1.2 of the IGN (considered to be "other enforceable means") requires a licence holder to comply with the AML/CFT Code.

manager, the IOMFSA may also impose under sec. 37(2) a penalty of such amount as considered appropriate on that individual.

443. Under the RBSA 2000, the IOMFSA's powers are limited to cancelling the administrator's registration. However, the IOMFSA is able to restrict (and effectively suspend) the business undertaken by an administrator through its regulation of retirement benefit schemes, where it will not authorise such a scheme unless it is satisfied with the administrator.

444. The IOMFSA may also apply administrative sanctions under the CIS 2008. In particular: (i) sec. 10 allows it to direct that an individual is unfit to be appointed, or continue as a director, controller or key person; (ii) sec. 11A and 11B allow it to direct that a member of the governing body is unfit to be appointed or continue to be appointed, or prohibit a person from becoming or continuing in such a role; (iii) sec. 12 allows it, amongst other things, to issue a direction to suspend the operations of a CIS, conduct a special audit or wind up the CIS; and (iv) sec. 14(6) allows it to issue a public notice about any direction, appointment, withdrawal, variation, termination or refusal.

445. The DBRO Act contains a variety of administrative sanctions that may be applied to other FIs and DNFBPs. In particular: (i) sec. 9 allows it to place conditions on registration; (ii) sec. 11 allows it to revoke a registration; (iii) sec. 26 allows it to issue written directions which can require action to be taken including that any business carried on by that FI is in whole, or in part, suspended or discontinued; (iv) sec. 27 allows it to issue a public statement; (v) sec. 29 allows it to seeking injunctions and a remedial order for contravention of, inter alia, AML/CFT requirements; and (vi) sec. 30 allows it to issue financial civil penalties. Penalties are set out in the Designated Businesses (Civil Penalties) Order 2015, and include a penalty of GBP 5 000 for carrying on unauthorised business and GBP 1 000 for failing to comply with a registration condition or direction.

446. The IOMFSA is also able to apply to the court for an injunction under sec. 20 of the FSA 2008 and for an injunction or remedial order under sec. 38 and 39 of the IA 2008. These are considered to be civil sanctions.

447. Failure to comply with the AML/CFT Code is a criminal offence under para. 41. A person who contravenes the AML/CFT Code is liable, following a trial, on conviction to a custodial sentence not exceeding 2 years, or an unlimited fine, or both. The decision and power to prosecute under the AML/CFT Code rests with the Attorney General.

448. The IOMFSA has explained that it does not automatically refer cases where it is to take regulatory action in order to determine whether there is sufficient evidence to take criminal action. It has explained that it would look at a number of factors, such as the degree of the breach, result of the breach, and the intent/ lack of intent when deciding whether to refer a case to the AGC.

Online gambling operators

449. Limited administrative powers are available to the GSC under the OGRA 2001. Under sec. 13, Commissioners shall cancel a licence where, after consultation with the Treasury, they are satisfied that the holder would not be eligible to be granted a licence on one or more of the grounds specified in sec. 4(2) (including integrity of the licence holder and management thereof)[109]. The GSC may also suspend or cancel a licence (without reference to the Treasury) under this sec. in a number of cases, including where an online gambling operator has failed to comply with any requirement of the Online Gambling Code. Sec. 15 also allows the GSC to direct, by notice to the holder, that a person be removed from their position as a director, or deprived of any managerial functions, as the case may be, where any director of the holder of a licence, or any other person who exercises managerial functions with respect to the conduct of online

[109] The GSC is not bound to take account of Treasury input.

gambling authorised by a licence, is not a suitable person to act as a director of the holder of the licence, or to exercise such functions.

450. In particular, the GSC does not have administrative fines at its disposal to promote compliance by online gambling operators with the AML/CFT regime. This has a significant negative impact on the assessment of proportionality of the sanctions available.

451. Failure to comply with the Online Gambling Code is a criminal offence under para. 22. A person who contravenes the Code is liable, following a trial, on conviction to a custodial sentence not exceeding 2 years or to an unlimited fine, or to both.

Casinos

452. One administrative power is available to the GSC. Sec. 5 of the CA 1986 permits the GSC to suspend or revoke a licence at any time if it is satisfied that it would be precluded from renewing a casino licence or empowered to refuse a licence for the reasons set out in sec. 5(6), which include failing without reasonable excuse to comply with the conditions of a licence. Since 1 February 2016, the casino's licence has included the following condition: "The licensee shall comply with the provisions of the Anti-Money Laundering and Countering the Financing of Terrorism requirements (AML/CFT)".

453. Sec. 4 of the CR 2011 requires the GSC to hold an inquiry, where it appears that there are, or may be, reasonable "grounds of complaint" to justify the revocation or suspension of a licence. As soon as practicable after holding such an inquiry, the GSC must cause notice in writing of its decision, with reasons for it, to be sent to the holder of the licence. The insular authorities have advised the evaluation team that it is unclear whether a complaint from the GSC's inspectors relating to AML/CFT matters would be an acceptable complaint to trigger an inquiry.

454. Administrative fines are not at the disposal of the GSC to promote compliance by the casino with the AML/CFT regime. This has a significant negative impact on the assessment of proportionality of the sanctions available.

455. Failure to comply with the AML/CFT Code is a criminal offence under para. 41 of the AML/CFT Code (see above).

NPOs

456. As described in the 2009 Report, CRA 1989 provides for criminal penalties on trustees, directors, managers or similar officers, who breach the statutory obligations (para. 926). SNPOs can be sanctioned for failure to comply with the AML/CFT obligations under para. 41 of the AML/CFT Code.

All

457. Where a person fails to make a report under sec. 142 to 144 of the POCA 2008, they are liable, following a trial, under sec. 150 to a custodial sentence not exceeding 2 years, or an unlimited fine, or both. Similar fines are set out in the ATCA.

458. Where a person commits a tipping-off offence under sec. 145 of the POCA 2008, they are liable, following a trial, under sec. 145(4) to a custodial sentence not exceeding 2 years, or an unlimited fine, or both. There is no tipping-off offence under the ATCA.

459. Failure to comply with legislation implementing targeted financial sanctions related to terrorism and TF may result in a custodial sentence not exceeding 2 years, or an unlimited fine, or both. Offences are set out in: the Al-Qaida Regs. 2013 (UNSCR 1267/1989); the Afghanistan Sanctions Regs. 2012 (UNSCR 1988); and the European Communities (Terrorism Measures) (Enforcement) Regulations (UNSCR 1373). Similar types of penalties are also set out in the TOCFR (UNSCR 1373).

460. *Criterion 35.2*. (Mostly met) - The range of administrative sanctions described above that is applicable to FIs and DNFBPs includes sanctions that are applicable also to directors and senior management – except for DNFBPs that are supervised under the DBRO Act where sanctions may be applied only against the registered entity. As noted under c.35.1, whereas it is possible to apply civil penalties to directors and senior management under the IA 2008, this is not also possible under the FSA 2008[110].

461. Para. 41 of the AML/CFT Code applies criminal sanctions to FIs, DNFBPs and SNPOs (who are natural persons or bodies corporate). Para. 41(4) extends the offence to directors and senior management where the officer is guilty of consent, connivance or neglect in relation to the offence. Para. 22(4) of the Online Gambling Code includes similar provisions. Legislation implementing targeted financial sanctions related to terrorism and TF applies sanctions to directors and senior management where the officer is guilty of consent, connivance or neglect in relation to the offence. In addition, directors found not to be fit and proper can be disqualified from acting as directors under the IoM companies legislation.

Weighting and Conclusion

462. The IoM mostly meets c.35.2 and partly meets c.35.1. **R.35 is rated partially compliant**.

Recommendation 36 – International instruments

463. In the 2009 Report, the IoM was rated partially compliant with former R.35 and SR.I. Assessors found that UK ratification of the Palermo Convention had not been extended to the IoM and not all provisions of the Palermo Convention, Vienna Convention and Terrorist Financing Convention were fully implemented.

464. *Criterion 36.1.* (Met) - As a British Crown Dependency, the IoM is not empowered to sign or ratify international conventions on its own behalf but, following a request by the IoM Government, UK's ratification of conventions was extended to the IoM.[111]

465. *Criterion 36.2* (Mostly Met) - When an international instrument is extended to the IoM by the UK, whilst the IoM is domestically responsible for its implementation the UK remains ultimately responsible to the relevant treaty for compliance with the instrument.

466. The IoM has implemented most of the Vienna Convention's provisions relevant to the FATF Recommendations. However, the deficiency noted in the 2009 IMF report with respect to extraterritoriality remains valid.

467. Regarding the implementation of the TF Convention, the deficiencies identified in the 2009 IMF report in the IoM's FT criminalisation have been addressed by the Anti-Terrorism and Crime (Amendment) Act 2011. At the same time, IoM law provides that acts undertaken or threats made with the intention of advancing a political, religious, racial or ideological cause would constitute "terrorism". This approach, which adds an element not set forth directly in the TF Convention, is adopted to ensure that the generic definition of terrorism is not used in circumstances where it was not intended. The authorities should assess the advantage of this approach in implementing the Convention, and ensure that the IoM's ability to prosecute in factual settings contemplated by the Convention will not be negatively impacted. This mental element does not apply to any activity which would constitute a "Convention offence"[112].

---

[110] Where a designated business is an individual, sanctions may be applied against that individual in their capacity as a registered entity.

[111] Conventions ratified by the UK extend to the IoM: Vienna Convention (02/12/93); TF Convention (25/09/08); Merida Convention (09/11/09); and Palermo Convention (01/07/12). Except in the case of certain categories of bilateral agreements (such as tax information exchange agreements) where the IoM is "entrusted" to do so by the UK.

[112] "Convention offence" is defined in sec. 75 of ATCA as an offence listed in Schedule 13A of the Act or an equivalent offence under the law of a country or territory outside the IoM.

468. As regards implementation of the Palermo Convention, in the 2009 Report the assessors found that the IoM had partly implemented the FATF Recommendations. Therefore, improvements in the laws were required in self-laundering for the acts of acquiring, possessing, or using criminal proceeds, and in the measures taken for the confiscation of proceeds of crime and instrumentalities used/intended for use in the crime, so as to comply fully with all provisions of the Convention.

469. In addition, the 2011 ATCA (Amendment) inserted several new provisions into sec. 10 of the ATCA, addressing the concerns related to the requirements of proof for the material elements of the ML offences, which formulated in its 2009 Report. Respectively, the deficiency identified in its 2009 Report related to the defence of payment of an 'adequate consideration' has been addressed. Nonetheless, as regards the confiscation of "laundered property", the situation remains mainly unchanged since the previous assessment (see analysis under Recommendation 4, criterion 4.1(a)).

470. Measures have been taken to bring IoM law in line with the provisions of the Merida Convention, in particularly with the enactment of the Bribery Act 2013.

Weighting and Conclusion

471. The IoM meets c. 36.1 and mostly meets c. 36.2. **R.36 is rated largely compliant**.

Recommendation 37 - Mutual legal assistance

472. In the 2009 Report, the IoM was rated PC with former R.36 and S.R. V due to the non-extension to the IoM of ratification of the Palermo Convention and the partial implementation of the Palermo and Vienna Conventions' provisions. Also deficiencies in criminalisation of TF affected its MLA capacity where the dual criminality principle applies. Availability of MLA related to seizure and confiscation was limited to 'designated' countries and equivalent value confiscation was not provided for in TF matters (also relevant in international cooperation context). These deficiencies have been partially addressed according to description provided under Recommendations 5, 6 and 36.

473. *Criterion 37.1.* (Met) - The IoM has a legal basis that allows its authorities to rapidly provide a wide range of MLA in relation to ML, associated predicate offenses and TF investigations, prosecutions and related proceedings. The legal basis for the provision of a full range of MLA is not confined to one law, although the advent of POCA 2008 and its secondary legislation, specifically, the Proceeds of Crime (External Investigations) Order 2011 (POCEI 2011) has updated and streamlined the IoM's approach to international cooperation in criminal matters. The CJA 1991 and Proceeds of Crime (External Investigations) Order 2011 (POCEI 2011) supplement the main legal framework for MLA. The UK has concluded nine bilateral MLA treaties that have been extended to the IoM. In addition to the more formal methods outlined below, the Central Authority for MLA in the IoM, the AGC, and the International Cooperation Team at the FCU provide assistance in facilitating voluntary interviews and witness statements, as well as the use of facilities at the IoM Court for witnesses to give evidence in trials in other jurisdictions via video link.

474. *Criterion 37.2.* (Mostly Met) - The AGC is the Central Authority in the IoM for the transmission and execution of MLA requests. All incoming and outgoing requests are dealt with by one full-time, legally qualified employee and are prioritised in terms of urgency. There are no formal rules in processing MLA requests. A file review is undertaken by the Legal Officer who has been co-opted into the Crown Office and reports directly to the Solicitor General, with whom all MLA requests are considered upon receipt.

475. *Criterion 37.3*. (Met) - The POCA 2008 and POCEI 2011 set out the general framework applicable to MLA and it does not appear to be prohibited or made subject to unreasonable or unduly restrictive conditions. Although dual criminality is required, the conduct underlying the

offence, rather than the terms in which it is expressed in the legislation of the requesting country, is considered in assessing whether this requirement is met.

476. *Criterion 37.4.* (Mostly Met) - Sec. 21(7) of CJA sets out the limited circumstances where assistance cannot be given under sec. 21 due to the fiscal nature of the relevant offences.[113] The authorities claim that such a situation could arise only rarely, and there have been no instances of a request being refused on this ground within the last five years. Assistance under sec. 30 of the CJA 1991, sec. 24 of the CJA 1990, the POCA 2008 and the POCEI 2011 is not precluded by the presence of fiscal elements in the relevant offences. The IoM does not have an overarching policy or regime of banking secrecy. Witnesses from banks, TCSPs and online casinos are summoned to give evidence and witness statements on a monthly basis. Sec. 7 of the Bankers' Books Evidence Act 1935 specifically provides for banking records to be produced when ordered by a judge, confidentiality notwithstanding.

477. *Criterion 37.5.* (Met) - Confidentiality of MLA requests and the information contained therein is maintained throughout the process. Only the FCU and the High Bailiff (or other judge to whom an application for execution of the request is made) have sight of the ILOR. ILORs are not disclosed to witnesses (or anyone else) at any stage. Court hearings for the taking of evidence and witness statements are held in private. Case law concerning MLA in the IoM upholds this approach. Legal Officers have a duty of confidentiality, as well as all civil servants, including officers of the Attorney General's Chambers are required to sign a declaration[114] under the Official Secrets Act 1911 (as amended).

478. Confidentiality of ILORs may be compromised where restraint or confiscation orders made in response to an MLA request are challenged. In the first instance, the restraint order is made, or the foreign confiscation order registered in the IoM, without notice to the defendant. However, once the order is made, notice is required to be served upon the defendant and they may appeal against the making of the order. During those proceedings, disclosure of ILORs is likely to be sought.

479. *Criterion 37.6* (Met) - Dual criminality is required only for coercive investigative processes, such as search and seizure, and the conduct underlying the offence, rather than the terms in which it is expressed in foreign legislation, is considered in assessing whether dual criminality exists.

480. *Criterion 37.7* (Met) - As described at c. 37.6, the conduct underlying the offence, rather than the terms in which it is expressed in foreign legislation, is considered in assessing whether dual criminality exists.

481. *Criterion 37.8* (Met) - Specific MLA methods and domestic provisions relating to the garnering of information, witness statements and documentary evidence (including banking and fiduciary records), service of judicial documents, searches, restraint and confiscation are extended to use in executing ILOR. Under the POCEI 2011 investigative mechanisms such as production orders can also be used in response to a request for MLA.

Weighting and Conclusion

482. The IoM meets c. 37.1, 37.3 and 37.5 - 37.8, mostly meets c. 37.2 and c. 37.4. **R.37 is rated largely compliant**.

[113] These are: (i) criminal proceedings have not yet been instituted; (ii) the request is from a non-Commonwealth country and is not made pursuant to a treaty to which the UK is a party and which extends to the IoM; and (iii) there is no dual criminality.

[114] Breaching the Act is an offence.

Recommendation 38 – Mutual legal assistance: freezing and confiscation

483. In its 2009 Report, IoM was rated PC with the former R.38 and SR.V. Assessors found regarding R.38 that deficiencies in the ML criminalization affected the MLA capacity where the dual criminality principle applies. Also, availability of MLA related to seizure and confiscation limited at time of assessment to 'designated' countries.

484. *Criterion 38.1* (Met) - Sec. 215 of POCA 2008 provides for the making of secondary legislation to enable restraint orders made outside the IoM to be enforced in the IoM. In addition, Chapter 1 of Part 3 of POCER 2009 deals with external requests for restraint of property. The AG may process an external request in connection with criminal investigations or proceedings in the requesting country and concerning relevant property, proceeds of, instrumentalities used in or intended for use in crime, and property of corresponding value. The requirement is to show that there is reasonable cause to believe that the alleged offender has benefitted from his criminal conduct, not to show a direct link between the property and the offence.

485. Although dual criminality is required, as outlined at c. 37.3, no such circumstances have arisen since the introduction of POCER 2009.

486. *Criterion 38.2* (Met) - Powers in Part 1 of POCA 2008, in conjunction with the POCER 2009, allow for the enforcement of foreign non-conviction based confiscation orders and in the case of MLA, it is immaterial whether criminal proceedings have been brought in the country making the request. The investigative mechanisms under POCA 2008 and the POCEI 2011 can also be used to provide MLA in response to a non-conviction based confiscation investigation. The POCER 2009 provides for the AGC to apply to the High Court for a property freezing order, either before or after starting civil recovery proceedings, in order to preserve the property in anticipation of the recovery order.

487. *Criterion 38.3* (Partly Met) - There are no formal arrangements for coordinating seizure and confiscation actions with other countries. Arrangements are made on a case by case basis with liaison between the Legal Officer, International Cooperation at the AGC, the FCU and the requesting jurisdiction. The IoM has mechanisms for managing, and when necessary disposing of, property frozen, seized or confiscated. Art. 64 of the POCER 2009 provides for the appointment of management receivers in respect of property specified in the restraint order and the court can confer a full range of powers upon them under Art. 65. Due to the predominance of the financial sector in the IoM, most of the assets frozen in response to MLA requests are bank accounts or other financial products which require no management (or are effectively managed by their provider). Extant restraint orders are reviewed by the Legal Officer, International Cooperation and updates as to the progress of the investigation or proceedings in the requesting jurisdiction sought. If the investigation is discontinued, or no conviction results from the proceedings, the AGC makes an application for the restraint order to be discharged. In the event of conviction, a request for confiscation follows. In respect of confiscation for MLA purposes, the relevant provisions are Art. 75 and 76 of the POCER 2009, which deal with the appointment of and powers of enforcement receivers. In civil recovery proceedings brought in response to a request for MLA, if a property freezing order is made Art. 14 – 16 of POCER 2009 provide for appointment and powers of receivers. In cases where an interim receiving order is made, Art. 18 of POCER 2009 deals with the functions of the interim receiver.

488. *Criterion 38.4* (Met) – The IoM is able to share confiscated property under sec. 222(4) of POCA 2008. Asset sharing is dealt with under this provision on a case by case basis, with factors such as the extent and complexity of the assistance provided taken into account with priority given to any victims' losses.

Weighting and Conclusion

489. The IoM meets c.38.2 and 38.4. It partly meets c.38.1 and 38.3. **R.38 is rated largely compliant.**

Recommendation 39 – Extradition

490. In the 2009 Report, the IoM was rated LC with the former R.39 and SR.V. Assessors found that deficiencies in the criminalisation of ML affected extradition capacity where the dual criminality principle applies. Deficiencies regarding SR.V are described under R.37.

491. *Criterion 39.1* (Met) - The terrorism related ML offence defined in ATCA sec. 10 and the ML and related offences set out in Part 3 of POCA 2008 are generally punishable by custody of 14 years or more and therefore qualify as an extraditable offence within the scope of the Extradition Act (EA) 1989. The extradition regime in the IoM is governed primarily by the UK's Extradition Act 1989, sec. 29 of which provides that Parts I to V extend to the IoM, and have effect as if it were a part of the UK. Also, Part III of the Act contains the machinery for processing requests for extradition from foreign states with which the UK has extradition arrangements, including designated Commonwealth countries and Convention States to the European Convention on Extradition (ECE) 1957. No formal extradition procedures have ever been initiated, though the IoM has come close in recent years. Counsel's opinion has been taken and the AGC are satisfied that there is an effective and clear system in place in the event that the IoM were ever to receive or be required to initiate a formal extradition request. The IoM relies on the extradition case management system set up in UK legislation which is extended to IoM. There are no unreasonable or unduly restrictive conditions that would inhibit the execution of any extradition request. This applies to both the procedure and substance of any such request.

492. *Criterion 39.2* (Met) - As in other common law jurisdictions, there is no legal obstacle to the IoM extraditing its own nationals. In the event of the IoM refusing to extradite, it would be cognisant of Art. 6(2) of the ECE, and would endeavour to take over the prosecution from the requesting State. In that case, the IoM would also coordinate with the requesting jurisdiction to ensure the efficiency of the prosecution (Art. 12 of the Convention). In dealing with an incoming extradition request, the procedures outlined in Part III of the EA would need to be followed in respect of the provisional arrest of the person to be extradited, habeas corpus, return of the person, simplified procedures, etc. In principle, the procedure provisions do not appear to contain unreasonable delay elements. TF is criminalised by sec. 7 to 10 of ATCA and offences are all punishable upon conviction on information by custody for a term not exceeding 14 years (or an unlimited fine or both) and are therefore extraditable offences within the scope of the EA and the Convention. Extradition based on such conduct would follow the same principles and procedures as with those related to ML described above. Sec. 14 of the EA provides for the possibility of simplified extradition procedures when the person who is the subject of the extradition request waives his rights.

493. *Criterion 39.3* (Met) - Dual criminality is a prerequisite for extradition to another jurisdiction, although assessed on the substance of the facts rather than on the basis of a formal qualification. This principle is imbedded in sec. 2 of the EA requiring the criminal conduct underlying the foreign extradition request also to be an offence in the UK (read Isle of Man), punishable with imprisonment of 12 months or more. It is then irrelevant how the criminal facts are described in the law of the requesting State.

494. *Criterion 39.4* (Met) - No simplified extradition mechanism is in place. The current extradition regime in the IoM is simple. However, it is to be hoped that a new IoM extradition regime will be introduced in the form of a pending Extradition Bill, the effect of which will be to locate much more of the procedural steps within the actual territory of the IoM itself.

Weighting and Conclusion

495. The IoM meets criteria 39.1 -39.4. **R.39 is rated compliant.**

Recommendation 40 – Other forms of international cooperation

496. In its 2009 Report, the IoM was rated compliant with R.40.

497. *Criterion 40.1* (Met) - Legislation allows for a wide range of information to be exchanged with foreign authorities in relation to ML, associated predicate offences and TF, and there is no legal impediment to information being exchanged rapidly, spontaneously and upon request.

498. *Criterion 40.2* (Mostly Met) - The competent authorities have an extensive legal basis for providing cooperation.[115] There are no impediments to cooperation. All authorities use clear and secure gateways, mechanism or channels, e.g. use of the Egmont Secure Web by the FIU and Interpol network by LEAs. There are no formal rules directing the method by, or timeframes in which, MLA requests should be executed by the AGC. Requests are dealt with as speedily as possible, taking into account AGC and court resources, and the time required by witnesses for preparation. Although no clear guidelines exist, the AGC gives priority to requests for restraint of criminal assets (or suspected criminal assets). The authorities state that processes for the prioritisation and timely execution of requests are in place at IOMFSA, which aims to execute all requests within 28 days of receipt. No formal processes for information shared requests exist in law with respect to the GSC. It remains unclear whether the FIU has relevant processes to prioritise and respond to requests on a timely basis. The competent authorities have clear processes for safeguarding the information received. The FIU stores specific information, such as information received from foreign FIUs, on the secure police computer (see also c.29.6). Physical access to the FIU information is restricted to authorised staff.

499. *Criterion 40.3* (Met) - Competent authorities do not need an MOU to provide assistance, though they have established bi-lateral and signed up to multilateral MOUs when appropriate.

500. *Criterion 40.4* (Met) - Upon request, the IoM competent authorities would provide feedback on the use and usefulness of the information obtained to any competent authority from which it had received assistance.

501. *Criterion 40.5* (Met) - The competent authorities do not prohibit or place unreasonable or unduly restrictive conditions on information exchange or assistance, and do not refuse requests for assistance on any of the four grounds listed in this criterion.[116]

502. *Criterion 40.6* (Met) - The competent authorities have in place controls and safeguards to ensure that information exchanged is used only for the intended purpose, unless prior authorisation has been given by the requested authority.[117]

503. *Criterion 40.7* (Met) - Competent authorities of the IoM maintain appropriate confidentiality with regard to requests for information received, consistent with privacy and data protection requirements and with confidentiality rules that are applied to information received from domestic sources. Information exchanged should also be subject to confidentiality by the requesting foreign authority. In general, the IOMFSA, the customs authorities, the FIU and police

---

[115] **CED**: CEMA 1986, Sec.174B to 174D, Sec.3, 3A, Schedule 3A; C&E (Implementation of 1979 Agreement) Order 1980, Art.7; Sec.77A and Schedule 12 of VAT Act 1998, EU Regulation 515/97/EC and the EU Mutual Assistance and Recovery Directive, EU Regulation 904/2010/EU; Sec.58 of ATCA; Sec.34 of the TOCFR 2014; **IOMFSA**: Sec.34 of FSA 2008, Schedules 5,6 of the IA 2008; **GSC**: Sec.6 and Schedule 2 of the Gambling Supervision Act 2010; Schedule 1 of the GA 1984; **FIU**: Parts 1 (ch.3), 2, 6, Sec.210 (3) and (4), Sec.213, 214, 218 of the POCA 2008; Sec.57 of the ATCA.

[116] Additional information on provision of assistance regardless of possible involvement of fiscal matters and existence of secrecy and confidentiality laws can also be found in para 1033-1036 of the 2009 Report.

[117] Also see c.40.2 above and para.1037-1039 of the 2009 Report.

maintain strict confidentiality in respect of any request for co-operation and information exchange.[118]

504. *Criterion 40.8* (Met) - Competent authorities can conduct inquiries on behalf of their foreign counterparts, and exchange all information that would be obtainable by them if such inquiries were being carried out domestically. Specific inquiries and information exchanges relating to AML/CFT are handled by the FIU. The IOMFSA and Customs and Excise also have broad powers in legislation and relevant international agreements to conduct inquiries on behalf of their foreign counterparts and exchange information on the relevant matters.[119]

505. *Criterion 40.9* (Met) - The FIU exchanges information with foreign FIUs in accordance with the Egmont Group principles or under the terms of the relevant MOU, irrespective of the nature of the counterpart FIU. All FIU ML/FT-related requests are handled by the FIU, more specifically by its international cooperation team. The legal basis for providing cooperation is described in c. 40.2(a).

506. *Criterion 40.10* (Mostly Met) - The FIU does not routinely receive any requests from other jurisdictions for feedback on information provided. Similarly the FIU has not until recently sought feedback on outcomes resulting from information provided, however work is underway to embed routine feedback.

507. *Criterion 40.11* (Met) - The FIU is authorised to exchange all information required to be accessible or obtainable directly or indirectly by the FIU (in particular under R.29), and any other information which it has the power to obtain or access, directly or indirectly, at the domestic level, subject to the principles of reciprocity. The FIU has a wide range of powers to collect information from financial, administrative and police powers.

508. *Criterion 40.12* (Mostly met) - Sec. 34(3) of the FSA 2008 allows the IOMFSA to exercise powers conferred on it by that Act for the purpose of investigating any circumstances referred to in a request from a regulatory authority with which the IOMFSA has a mutual assistance agreement[120]. Sec. 34(2) of the FSA Act also permits spontaneous exchange of information by the IOMFSA where it has a mutual assistance agreement with an overseas regulator. Furthermore, paragraph 2(5) of Schedule 5 permits the disclosure of information by the IOMFSA on request to an overseas regulatory authority where information disclosed relates to the IOMFSA's regulation and supervision of persons undertaking regulated activities. Based on these provisions assistance could be provided.

509. *Criterion 40.13* (Mostly met) - The IOMFSA is able to exchange with foreign counterparts information domestically available to it including information held by FIs using the powers and gateways set out under c.40.12, specifically using the powers of inspection and investigation provided in Schedule 2 of the FSA 2008 and Schedule 5 of the IA 2008 and the gateways of disclosure set out in Schedule 5 of the FSA 2008 and Schedule 6 of IA 2008.

510. *Criterion 40.14* (Mostly met) - When relevant for AML/CFT purposes, the IOMFSA is in a position to exchange: (i) regulatory information; (ii) prudential information; and (iii) AML/CFT information.

---

[118] **ITD**: Official Secrets Acts 1911 and 1920; Data Protection Act 1998; EU Directive 95/46/EC; Council of Europe Convention 108 for the Protection of Individuals; EU Directive 2003/48/EEC; **the IOMFSA**: Schedule 5, para.1(2); **the FIU/Police:** the IoM Government Corporate Information and Records Policy 2011; sec. 210-214 POCA 2008; sec. 56-57 ATCA, DPA 1998 and internal LEAs policies and procedures – Police Regulations 2015; Civil Service Regulations; the Egmont Group Principles.

[119] **ITD**: Sec. 104H,I, 105C to 105O of ITA 1970; GSC: Sec. 6 of the GSA Act 2010; **IOMFSA:** Sec. 15 and Schedule 2 and 5 of FSA 2008 and Schedule 5 and 6 of the IA 2008; **LEAs:** direct bilateral contacts, the Interpol Network.

[120] The FSA is a full signatory to the IOSCO Multilateral MOU and signatory to the IAIS Multilateral MOU. The IOMFSA has entered into 27 Co-operation Agreements under the EU's Alternative Investment Fund Managers Directive. In addition, the IOMFSA has 40 regulatory and supervisory MOUs.

511. *Criterion 40.15* (Mostly met) - The IOMFSA is able to conduct inquiries and investigations on behalf of foreign counterparts using its powers under sec. 34 and Schedule 2 FSA 2008 and exchange with foreign counterparts under Schedule 5 all information that would be obtainable by them if such inquiries were being carried out domestically. However, the FSA may not always be able to provide assistance under the DBRO Act to an overseas regulator.

512. *Criterion 40.16* (Met) - Information received by the IOMFSA from foreign supervisory authorities may only be passed on with the consent of the authority concerned and only for the purposes for which the consent was given: Schedule 5 para 192 of the FSA 2008. There are similar provisions in other legislation.

513. *Criterion 40.17* (Met) - The FCU is permitted to internationally exchange information for both intelligence and investigative purposes through direct bilateral contacts and use the international communication network of Interpol, as long as it does not involve coercive measures, such as taking voluntary witness statements and conducting informal enquiries. The use of coercive and invasive measures to collect evidence, particularly in the form of financial information and documents of a confidential nature, requires judicial review and assent, and in that case assistance can only be given on a MLA basis. The C&E is able to co-operate with a large number of foreign countries in customs-related matters under mutual assistance agreements between those countries and the EU. Cooperation with countries outside the scope of these agreements is conducted on a case-by-case basis.

514. *Criterion 40.18* (Met) - The LEAs (the FCU and Customs and Excise) may use their powers and investigative techniques to conduct inquiries and obtain information on behalf of their foreign counterparts. The IoM cooperates with foreign counterparts based on direct bilateral contacts and multilateral agreements in the context of Interpol.

515. *Criterion 40.19* (Met) - The LEAs are able to form joint investigative teams with their foreign counterparts to conduct cooperative investigations, and, when necessary, establish bilateral or multilateral arrangements to enable such joint investigations.

516. *Criterion 40.20* (Met) - The FIU, LEAs (the FCU and Customs and Excise), and IOMFSA are authorised to exchange information indirectly with non-counterparts.[121]

Weighting and conclusion

517. The IoM meets criteria 40.1, 40.3-40.9, 40.11, and c.40.16-40.20 and mostly meets c.40.2, c.40.10 and c.40.12-c.40.15. **R.40 is rated largely compliant.**

[121] **FIU/FCU**: Part 6 and Sec. 213 of the POCA 2008; **IOMFSA**: Schedule 5 of the FSA 2008; C&E: Sec. 3A and schedule 3A; sec. 174B and 174D, C&E Management Act 1986; sec. 31, Terrorism and Other Crimes (Financial restrictions) Act 2014; C&E (Implementation of 1979 Agreement) Order 1980 - for HMRC, NCA, UK Border Force; sec. 77A and Schedule 12, VAT Act 1996; sec. 58 ATCA; orders under Part 7, POCA 2008; various orders and regulations implementing UN or EU sanctions.

Summary of Technical Compliance – Key Deficiencies

Compliance with FATF Recommendations		
Recommendation	**Rating**	**Factor(s) underlying the rating**
1. Assessing risks & applying a risk-based approach	LC	• The IOMFSA, the FIU and law enforcement authorities should focus their activities in line with the risk profile of the country. • The NRA has been completed relatively recently and the AML/CFT regime has not yet been tailored entirely to fit the risks identified. • The exemptions from the full scale of CDD provided under Art. 21 of the AML/CFT Code are not based on a holistic consideration of the risk factors and variables mentioned in the Interpretative Note to R.10, most importantly when it comes to the risk profile of the underlying client. The scope of the exemption is not clearly limited. . • There is no specific requirement for risk assessments in the online gambling sector to be kept up-to-date and to provide risk assessments information to the GSC • There is no clear requirement to document and update risk assessments taking into consideration all necessary factors and that the policies, controls and procedures must be approved by senior management.
2. National cooperation and coordination	C	
3. Money laundering offence	C	
4. Confiscation and provisional measures	LC	• Absence of general provisions explicitly covering the confiscation of the property that is the proceeds of, used in, or intended or allocated for use in the financing of terrorism, terrorist acts or terrorist organisations.
5. Terrorist financing offence	LC	• The TF offence does not criminalise the financing of unproscribed terrorist organisations in the absence of a link to a specific terrorist act. • There are no specific TF offence provisions which would include financing the travel of individuals who travel to a State other than their States of residence or nationality for the purpose of the perpetration, planning, or preparation of, or participation in, terrorist acts or the providing or receiving of terrorist training.
6. Targeted financial sanctions related to terrorism & TF	LC	• For UNSCR 1373, the freezing obligation does not cover a sufficiently broad range of assets under the EU framework. • There are no publicly available procedures to deal with "false positives". • No guidance is available to financial sector and DNFBPs on obligations to respect de-listing or unfreezing action.
7. Targeted financial sanctions related to proliferation	LC	• The deficiencies identified under the supervisory regime apply under c.7.3. • Absence of clear provisions in the law with respect to requirements set out under c.7.5(b). • There are no publicly available procedures to deal with "false positives".
8. Non-profit organisations	LC	• The domestic analyses of the NPO sector did not take into account the non-charitable NPO sector. A reassessment of the NPO sector in the future should also encompass registered SNPOs. • The information from the Central Registry does not cover the data on the identity of the persons who own, control or direct the activities or on the assets at the disposal of the SNPOs. • There is no requirement for non-charitable SNPOs to make available information on their administration and management. It is not clear if the authorities have access to this information nor what would be the source of such information.
9. Financial institution secrecy laws	C	
10. Customer due diligence	LC	• There is no requirement to undertake CDD measures where there is suspicion of ML/TF. • Not all FIs are required to verify that any person purporting to act on behalf of an individual is so authorised or to identity and verify the identity of that person. • There is not a proven low risk of ML/FT for some CDD exemptions.

Compliance with FATF Recommendations		
Recommendation	**Rating**	**Factor(s) underlying the rating**
		• Not all FIs are required to obtain and hold information on classes of beneficiaries of a trust. • There is no requirement to obtain information that will enable identification of a beneficiary of a life policy designated by characteristics, class or other means at time of pay-out. • CDD requirements are not applied to beneficiaries of all investment related insurance policies. • There is no requirement for information about the beneficiary of a life policy to be taken into account when considering whether to apply enhanced CDD measures. Nor is there a requirement to identify or verify the identity of the beneficial owner of a beneficiary that is not an individual. • There is a requirement to freeze rather than terminate an existing business relationship where CDD measures cannot be applied. • CDD measures must be applied even if this can lead to tipping-off.
11. Record keeping	LC	• Accounts files, business correspondence, and results of analysis undertaken will not always be kept for at least 5 years following termination of a business relationship or after the date of an occasional transaction.
12. Politically exposed persons	LC	• There is no requirement to determine whether the beneficial owner of a beneficiary of a life policy that is not an individual is a PEP.
13. Correspondent banking	C	
14. Money or value transfer services	LC	• MVTS operators are not clearly required to include agents in their AML/CFT programmes.
15. New technologies	C	
16. Wire transfers	PC	• There is no requirement to ensure that transfers are accompanied by required beneficiary information. • There is no requirement to verify payer information in case of transactions less than EUR 1,000 or where there is suspicion of ML/TF. • The ordering institution is not prohibited from executing wire transfers that do not comply with requirements. • There is no requirement for intermediary institutions to take reasonable measures to identify cross-border transfers that lack information or to have risk-based policies and procedures for determining what to do with such transfers.
17. Reliance on third parties	LC	• Reliance may be placed on a group third party that is not regulated, supervised or monitored.
18. Internal controls and foreign branches and subsidiaries	LC	• Not all FIs are required to appoint a compliance officer at management level or to have an independent audit function. • There is no specific requirement for groups to have group-wide programmes against ML/TF. • There is no requirement to apply additional measures to mitigate ML/TF risks where a branch or subsidiary is prevented by law from applying necessary CDD measures.
19. Higher-risk countries	C	
20. Reporting of suspicious transaction	C	
21. Tipping-off and confidentiality	LC	• Tipping off offences are too narrowly set.
22. DNFBPs: Customer due diligence	LC	*All DNFBPs except online gambling operators* • Factors underlying R.10, 11, 12 and 17 apply. *Online gambling operators* • There is no mandated threshold for evidence of identity to be obtained on the placing of a deposit. (R.10) • There is no requirement to apply CDD measures in all cases where there is doubt about previously obtained data or suspicion of ML/TF. (R.10) • In case of a customer that is not an individual, there is a requirement only to take reasonable steps to verify the identity of a person purporting to act on its behalf. (R.10) • The definition of beneficial ownership in the Online Gambling Code does not include the natural person on whose behalf a transaction is being conducted. (R.10)

Compliance with FATF Recommendations		
Recommendation	**Rating**	**Factor(s) underlying the rating**
		• There is no requirement to ensure that reviews of existing records take account of higher risk categories of customer. (R.10) • There is no requirement to understand the nature of a customer's business. (R.10) • Whilst guidance is published on the application of CDD measures to legal persons and legal arrangements, there are no specific requirements in the Online Gambling Code. (R.10) • There is no clear requirement to apply CDD measures to existing customers. (R.10) • Enhanced CDD measures may be limited to taking reasonable measures to establish source of funds and source of wealth (even if other measures are more appropriate). (R.10) • CDD measures must be applied even if this can lead to tipping-off. (R.10) • There are some gaps in requirements to apply CDD to PEPs and to assess the risk of new technology. (R.12 and R.15)
23. DNFBPs: Other measures	PC	*All DNFBPs except online gambling operators.* • Factors underlying R.18 and R21 apply. *Online gambling operators* • There is no requirement to appoint a compliance officer or to have an independent audit function to test the system. (R.18) • There is no requirement for policies and procedures covering employee screening or on-going training to have regard to ML/TF risks or size of operator. (R.18) • There is no specific requirement for groups to have group-wide programmes against ML/TF nor specific requirements to deal with branches or majority-owned subsidiaries. (R.18) • There are no measures in placed to actively advise licence holders of any concerns in the AML/CFT weakness of other countries. • Tipping off offences are too narrowly set.
24. Transparency and beneficial ownership of legal persons	PC	• Guides and practice notes do not explain the process followed for obtaining and recording beneficial ownership information. • There has been no formal assessment of the threats presented specifically by legal persons established under Manx legislation. • Information held at the Central Registry on directors of 2006 companies may be up to one year out of date. • Limited partnerships are not required to register partnership deeds nor foundations required to register rules. • There is no register of general partnerships, nor is there a statutory requirement to record the partners of a general partnership. • Not all basic information must be maintained by legal persons within the IoM. • It is not clear when a change in a partner of a partnership becomes legally binding and enforceable and how such changes are reported to the partnership. • The Central Registry does not check the accuracy of basic information. • It cannot be determined that accurate, complete and current beneficial ownership information will be available for 1931 companies, limited partnerships or general partnerships. • There are gaps in the application of requirements to companies and partnerships that are dissolved or otherwise cease to exist. • The nominee status of shareholders that are licenced nominees is not recorded in the Central Registry. The identity of non-licenced nominators is not recorded in registers of shareholders or in the Central Registry. • The range of sanctions that can be applied by the FIU and law enforcement for failing to grant competent authorities timely access to information is not proportionate.
25. Transparency and beneficial ownership of legal arrangements	PC	• There is no explicit requirement placed on the trustee of an express trust that is governed by Manx law where the trustee is resident outside the IoM, or resident in the IoM but non-professional to obtain and hold information in line with c25.1. • There is no explicit requirement placed on TCSPs subject to the AML/CFT Code to obtain information on classes of beneficiaries.

Compliance with FATF Recommendations		
Recommendation	**Rating**	**Factor(s) underlying the rating**
		• There is no explicit requirement in the Trustee Act requiring trustees to hold basic information on regulated agents of, and service providers to, a trust. • Record-keeping requirements do not apply to professional trustees that are resident outside the IoM. • Not all trustees are required to disclose their status when entering into a business relationship or carrying out a one-off transaction. • The common law duty of confidentiality may prevent a trustee providing information to a FI or DNFBP. • The range of sanctions that can be applied by the FIU and law enforcement for failing to grant competent authorities timely access to information is not proportionate.
26. Regulation and supervision of financial institutions	LC	• Not all of the activities or operations listed in the FATF's definition of FI are regulated or supervised. • The IOMFSA cannot supervise compliance with AML/CFT requirements by the manager of a single exempt scheme (a private collective investment scheme). • The authorities have not provided evaluators with an explanation for the basis of a number licensing exemptions. • At the time of the onsite visit, the IOMFSA's basis for assessing sector and cross-sector risk had not been formalised. • The IOMFSA has not clearly articulated how the frequency and intensity of supervision takes into account the degree of discretion given to FIs in the application of the AML/CFT Code.
27. Powers of supervisors	LC	• Not all of the activities or operations listed in the FATF's definition of FI are regulated or supervised. • The IOMFSA is unable to compel every person who it has reason to believe holds relevant information to provide that information under the FSA 2008.
28. Regulation and supervision of DNFBPs	LC	• The GSC relies on licensing conditions to supervise online gambling operators and the IoM's casino for AML/CFT compliance. • Acting as a partner of a partnership is not regulated or supervised by the IOMFSA. • At the time of the onsite visit, the IOMFSA's basis for assessing sector and cross-sector risk had not been formalised. The IOMFSA has not clearly articulated how the frequency and intensity of supervision takes into account the degree of discretion given to FIs in the application of the AML/CFT Code.
29. Financial intelligence units	LC	• The strategic analysis conducted by the FIU is limited in nature.
30. Responsibilities of law enforcement and investigative authorities	C	
31. Powers of law enforcement and investigative authorities	C	
32. Cash couriers	LC	• Although the FIU established under the new FIU Act 2016 continues to receive cash declarations, as a separate organisation in its own right, it will require an order extending sec. 174B to it, and it is probable that an MOU will have to be agreed to formalise existing arrangements • There is no provision in the CEMA requiring Customs and Excise to maintain records on (a) declarations, (b) false declarations, and (c) ML/TF suspicions.
33. Statistics	LC	• No comprehensive for the collection and maintenance of statistics.
34. Guidance and feedback	LC	• The FIU does not routinely publish typologies drawn from its analysis of STRs. • Information has not been provided on feedback provided by all competent authorities.
35. Sanctions	PC	• Not all of the activities or operations listed in the FATF's definition of FI are regulated or supervised. • Limited administrative powers are available to the GSC. • Sanctions may not be applied to directors and senior management under the DBRO Act. • Civil penalties may not be applied to directors and senior management

Compliance with FATF Recommendations		
Recommendation	**Rating**	**Factor(s) underlying the rating**
		under the FSA 2008.
36. International instruments	LC	• CJA sets out the limited circumstances where mutual legal assistance cannot be given due to the fiscal nature of the relevant offences.
37. Mutual legal assistance	LC	• CJA sets out the limited circumstances where mutual legal assistance cannot be given due to the fiscal nature of the relevant offences.
38. Mutual legal assistance: freezing and confiscation	LC	• There are no formal arrangements for coordinating seizure and confiscation actions with other countries.
39. Extradition	C	
40. Other forms of international cooperation	LC	• In the case of the DBRO Act, the IOMFSA's function is limited to assessing compliance with IoM AML/CFT legislation only and there are no separate provisions dealing with mutual assistance (as there are in other law) which consequently might limit providing international cooperation to overseas regulator.

TABLE OF ACRONYMS

ACCA	Association of Chartered Certified Accountants
AGC	Her Majesty's Attorney General's Chambers
AML/CFT	Anti-money laundering/combating financing of terrorism
ATCA	Anti-Terrorism and Crime Act 2003
BIS	Bank of International Settlements
BNIs	Bearer negotiable instruments
BO	Business objects
CA	Companies Act 1986
CBO	Companies (Beneficial Ownership) Act 2012
CCTV	Closed Circuit Television
CDD	Customer Due Diligence
CED	Treasury Customs and Excise Division
CEMA	Customs and Excise Management Act 1986
CFT	Combating the Financing of Terrorism
CFSP	Customs Freight Simplified Procedure
CISA	Collective investment Schemes Act 2008
CJA	Criminal Justice Act 1991
CLA	Criminal Law Act 1981
CODA	Company Officers (Disqualification) Act 2009
CRA	Charities Registration Act 1989
CRS	Common Reporting Standard
CSPs	Money Corporate Service Providers
CTA	Common Travel Area
C&E	Customs and Excise Division
DBRO	Designated Business Registration and Oversight Act 2015
DHA	Department of House Affairs
DHSC	Department of Health and Social Care
DNA	Deoxyribonucleic Acid
DNFBP	Designated Non-Financial Businesses and Professions
DPA	Data Protection Act 2002
DTA	Drug Trafficking Act 1996
EC	European Commission
EU	European Union
FATCA	Foreign Account Tax Compliance Act
FATF	Financial Action Task Force
FCU	Financial Crime Unit
FIs	Financial institutions
FIS	Financial Intelligence Service
FIU	Financial Intelligence Unit
FSA	Financial Services Authority
FSB	Financial Stability Board
FSC	Financial Services Commission
FSRB	Financial Service Rule Book
GBP	Great Britain Pound
GDP	Gross Domestic Product
GSC	Gambling Supervision Commission
GSI	Governments Secure Intranet
HMRC	Her Majesty's Revenue and Customs
HNWI	High-net worth individuals
IA	Insurance Act 2008
IAIS	International Association of Insurance Supervisors
IAMLR	Insurance (Anti-Money Laundering) Regulation 2008
ICAEW	Institute of Chartered Accountants in England and Wales
IFAs	Independent financial advisors

IFC	Independent financial consultants
ILORs	Incoming letters or requests
IMF	International Monetary Fund
INTERPOL	International Police
IO	Immediate Outcomes
IoM	Isle of Man
IOMFSA	Isle of Man Financial Services Authority
IOSCO	International Organisation of Securities Commissions
IRISL	Islamic Republic of Iran Shipping Line
ITA	Income Tax Act 1970
ITD	Treasury Income Tax Division
LEA	Law Enforcement Agency
LLCs	Limited Liability Companies Act 1996
LOR	Letter of request
MER	Mutual Evaluation Report
MMOU	Multilateral Memorandum of Understanding
ML	Money Laundering
MLA	Mutual Legal Assistance
MLRO	Money Laundering Reporting Officers
MOU	Memorandum of Understanding
MSBs	Money service businesses
MVTS	Money or Value Transfer Services
NCA	National Crime Agency
NPO	Non-profit Organisation
NRA	National Risk Assessment
NSG	National Strategy Group
OECD	Organisation for Economic Co-operation and Development
OFAC	Office of Foreign Asset Control
OFT	Office of Fair Trading
OGRA	Online Gambling Regulation Act 2001
OLORs	Outgoing letters of request
PEP	Politically Exposed Person
PF	Proliferation Financing
POCA	Proceeds of Crime Act 2008
POCEI	Proceeds of Crime (External investigations) Order 2011
PPPA	Police Powers and Procedures Act 1998
RAO	Regulated Activities Order
RBSA	Retirement Benefit Schemes Act 2000
RCR	Religious Charities Regulations 1999
SAR	Suspicious Activity Report
SNPO	Specified non-profit Organisations
STR	Suspicious Transaction Report
TCSP	Trust and Corporate Service Providers
TF	Terrorist Financing
TFS	Targeted financial sanctions
TFQ	Timber Forecast Questionnaire
TIEA	Tax Information Exchange Agreements
TOCFR	Terrorism and Other Crime (Financial Restrictions) Act 2014
TSPs	Trust Service Providers
UBO	Ultimate beneficial owner
UK	United Kingdom
UKPC	United Kingdom Privy Council
UNCR	United Nations Security Council Resolution
VAT	Value-added tax
WMD	Weapons of Mass Destruction

www.coe.int/MONEYVAL

December 2016

Anti-money laundering and counter-terrorist financing measures

Isle of Man

Fifth Round Mutual Evaluation Report

This report provides a summary of the AML/CFT measures in place in Isle of Man as at the date of the on-site visit (25 April to 7 May 2016). It analyses the level of compliance with the FATF 40 Recommendations and the level of effectiveness of Isle of Man's AML/CFT system, and provides recommendations on how the system could be strengthened.