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 SUMM

Isle of Man

Fifth Round Mutual Evaluation Report

Executive Summary

1. This report provides a summary of the AML/CFT measures in place 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

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

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 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