September 2009
IMF Country Report No. 09/278

Isle of Man: Financial Sector Assessment Program Update—Detailed Assessment of Observance of AML/CFT

This Detailed Assessment of Observance of AML/CFT Report on the **Isle of Man** was prepared by a staff team of the International Monetary Fund as background documentation for the periodic consultation with the member country. It is based on the information available at the time it was completed in August 2009. The views expressed in this document are those of the staff team and do not necessarily reflect the views of the government of the Isle of Man or the Executive Board of the IMF.

The policy of publication of staff reports and other documents by the IMF allows for the deletion of market-sensitive information.

Copies of this report are available to the public from

International Monetary Fund ● Publication Services
700 19th Street, N.W. ● Washington, D.C. 20431
Telephone: (202) 623 7430 ● Telefax: (202) 623 7201
E-mail: publications@imf.org ● Internet: http://www.imf.org

Price: $18.00 a copy

International Monetary Fund
Washington, D.C.

ISLE OF MAN

DETAILED ASSESSMENT REPORT ON ANTI-MONEY LAUNDERING AND COMBATING THE FINANCING OF TERRORISM

AUGUST 5, 2009

INTERNATIONAL MONETARY FUND
LEGAL DEPARTMENT

Contents Page

ACRONYMS

AG	Attorney General
AML/CFT	Anti-Money Laundering and Combating the Financing of Terrorism
AML Code 2007	Criminal Justice (Money Laundering) Code 2007
AML Code 2008	Criminal Justice (Money Laundering) Code 2008
ATCA 2003	Anti Terrorism Crime Act, 2003
BCP	Basel Core Principles
CC	Criminal Code
CDD	Customer Due Diligence
CEMA	Customs and Excise Management Act 1986
CJA 1990	Criminal Justice Act 1990
CLA 1981	Criminal Law Act 1981
1931 Companies	Companies incorporated pursuant to the Companies Acts 1931-2004
2006 Companies	Companies incorporated pursuant to the Companies Act 2006
CPC	Criminal Procedure Code
CSP	Corporate Service Provider
DHA	Department of Home Affairs
DNFBP	Designated Non-Financial Businesses and Professions
DTA 1996	Drug Trafficking Act 1996
DTU	Drug Trafficking Unit
EC	European Community
EU	European Union
FATF	Financial Action Task Force
FCU	Financial Crime Unit (the IOM FIU)
FI	Financial institution
FIU	Financial Intelligence Unit
FSA 2008	Financial Services Act 2008
FSAP	Financial Sector Assessment Program
FSC	Financial Supervision Commission
FSRB	FATF-style Regional Body
FT	Financing of terrorism
GBP	Great Britain Pound
GSC	Gambling Supervision Commission
IA 1986	Insurance Act 1986
IA 2008	Insurance Act 2008
IAIS	International Association of Insurance Supervisors
IAMLR	Insurance (Anti-Money Laundering) Regulation 2008
IGN	Guidance Notes on Anti-Money Laundering and Preventing the Financing of Terrorism for insurers (Long Term Business) 2008
IOM	Isle of Man
IPA	Insurance and Pensions Authority
JAMLAG	Joint Anti-Money Laundering Advisory Group
KYC	Know your customer/client

LEG	Legal Department of the IMF
LLC	Limited Liability Company
MEF	Ministry of Economy and Finance
MFA	Ministry of Foreign Affairs
MFD	Monetary and Financial Systems Department of the IMF
MOU	Memorandum of Understanding
ML	Money laundering
MLA	Mutual legal assistance
MLRO	Money Laundering Reporting Officer
MMOU	IOSCO Multilateral Memorandum of Understanding
MVT	Money or value transfer
NPO	Nonprofit organization
OFAC	US Office of Foreign Assets Control
OG Code 2008	On-line Gambling Code 2008
OGR 2008	On-line Gambling Regulations 2008
PEP	Politically-exposed person
POCA 2008	Proceeds of Crimes Act 2008
PPPA 1998	Police Powers and Procedures Act 1998
PTC	Private Trust Company
ROSC	Report on Observance of Standards and Codes
SRO	Self-regulatory organization
STR	Suspicious Transaction Report
The 1991 Act	Criminal Justice Act 1991
The Regulation	EC Regulation 1889/2005 of the European Parliament and of the Council of 26 October 2005
TSP	Trust Service Provider
UK	United Kingdom of Great Britain and Northern Ireland
UN	United Nations Organization
UNSCR	United Nations Security Council Resolution
VAT	Value Added Tax

PREFACE

This assessment of the anti-money laundering (AML) and combating the financing of terrorism (CFT) regime of the Isle of Man (IOM) is based on the Forty Recommendations 2003 and the Nine Special Recommendations on Terrorist Financing 2001 of the Financial Action Task Force (FATF), and was prepared using the AML/CFT assessment Methodology 2004, as updated in February 2008. The assessment team considered all the materials supplied by the authorities, the information obtained on site during their mission from September 3–18, 2008, and other verifiable information subsequently provided by the authorities. During the mission, the assessment team met with officials and representatives of all relevant government agencies and the private sector. A list of the bodies met is set out in Annex 2 to the detailed assessment report.

The assessment was conducted by a team of assessors composed of staff of the International Monetary Fund (IMF) and experts acting under the supervision of the IMF. The evaluation team consisted of: Terence Donovan (LEG, team leader) and the following LEG consultants: Mr. Jean-Manuel Clemmer (Banque de France); Ms. Gabriele Dunker; Ms. Lisa Kelaart-Courtney; and Mr. Boudewijn Verhelst (Deputy Head of Belgian FIU). The assessors reviewed the institutional framework, the relevant AML/CFT laws, regulations, guidelines and other requirements, and the regulatory and other systems in place to deter and punish money laundering (ML) and the financing of terrorism (FT) through financial institutions and Designated Non-Financial Businesses and Professions (DNFBP). The assessors also examined the capacity, implementation, and effectiveness of all these systems.

This report provides a summary of the AML/CFT measures in place in the IOM at the time of the mission or shortly thereafter. It describes and analyzes those measures, sets out the IOM's levels of compliance with the FATF 40+9 Recommendations (see Table 1) and provides recommendations on how certain aspects of the system could be strengthened (see Table 2). The findings and data in the report have been updated to late-2008. The report also notes, mainly by way of footnote, some further significant developments which occurred prior to its finalization in August 2009.

The assessors would like to express their gratitude to the IOM authorities for their cooperation, hospitality, and the high standard of organization and support throughout the assessment mission.

EXECUTIVE SUMMARY

Background and Key Findings

1. The Isle of Man (IOM) is an international financial center of some significance based in particular on the provision of banking and insurance-related products to nonresidents; funds business has been a growing sector and the IOM has also licensed some online gambling businesses. For the resident population on the island of over 80,000 and with GDP of GBP1.6 billion[1], the financial services sector represents the single largest component of the economy (36 percent of GDP). The IOM has its own legal system and jurisprudence based on the principles of English common law. Standards of governance and transparency appear to be high. Much of the financial services business in the IOM is, directly or indirectly, UK-related and the IOM financial institutions, many of which are subsidiaries of UK banks, are substantial providers of liquidity to the UK money markets.

2. The IOM is recognized for the expertise developed in a range of international financial products. Other key reasons for the growth in recent years in the IOM's financial services sector include the legal system (which is similar to that in the UK), the stable political and regulatory systems, and the competitive tax regime. In that regard, the IOM authorities are placing increasing emphasis on international cooperation, including through working closely with the relevant OECD initiative and entering into tax information exchange agreements (TIEAs), of which 17 have been signed with other jurisdictions.

3. While the IOM government has not published an AML/CFT strategy, as such, a political commitment has been given by the IOM authorities, in correspondence with the FATF and in public statements, to adhere to the principles of the FATF Recommendations. The authorities informed the assessors that the IOM attaches the highest importance to having a robust and enforceable regime for the prevention of money laundering and for countering the financing of terrorism. It is significant that, in addition to the stated objectives of the Financial Crime Unit (FCU)—the IOM financial intelligence unit (FIU)—both of the main supervisory authorities (the Financial Supervision Commission (FSC) and the Insurance and Pensions Authority (IPA)) have been assigned legislative objectives related to the reduction in financial crime.

4. The IOM has substantially updated its AML/CFT legal provisions from 2007 to late-2008 to reflect the FATF Recommendations and to parallel the implementation in EU member states of the Third Money Laundering Directive. Relevant new legislation includes the Proceeds of Crime Act 2008 (POCA 2008), the revised AML Code of December 2008[2], the Insurance Act 2008 (IA 2008), the Insurance (Anti-Money Laundering) Regulations 2008, and insurance binding guidance notes[3] issued by the IPA, and the Financial Services Act 2008 (FSA 2008), FSC Rule Book Part 9[4], and also the relevant guidance in the FSC's Handbook 2008.

---

[1] 2005/6

[2] Which is secondary legislation and qualifies as a 'regulation' for purposes of this assessment.

[3] Which qualify as "other enforceable means" for purposes of this assessment.

[4] As footnote 2

5. While the IOM is a low-crime jurisdiction, some characteristics of the financial system point to an increased potential of abuse for ML or FT purposes, as more than 90 percent of the business, often established through introducers, is conducted on a non face-to-face basis for nonresidents, and services provided include private banking and the use of legal persons and arrangements such as trusts, which have the potential to create an additional challenge in fulfilling the requirement to identify accurately the customer and the ultimate beneficial owner. The IOM's relevant legislation, regulation, and guidance are drafted with this in mind.

6. The IOM is broadly compliant with most aspects of the FATF Recommendations, having upgraded its AML/CFT requirements significantly, particularly in the second half of 2008.

7. Money laundering is criminalized broadly in line with the international standard and many, albeit not all, technical aspects of the Vienna and Palermo Conventions are complied with. All categories of predicate offences listed in the international standard are covered. While the statutory sanctions for ML-related offences are, in a formal sense, comprehensive, dissuasive, and proportionate, the sentences actually imposed by the courts appear rather low. At the time of the assessment, the IOM reported no convictions for autonomous money laundering with few domestic investigations or prosecutions. Financing of terrorism (FT) is criminalized under IOM law but the definition of the offence needs to be broadened. There were no convictions for FT-related offences.

8. Although a few deficiencies are identified in this report, the IOM's legal framework underpinning the seizure and confiscation system related to proceeds of crime is generally solid and comprehensive. The IOM should, however, develop case law on stand-alone money laundering confiscation and address the low effectiveness of the current asset recovery measures. The implementation by the IOM of UNSCRs 1267 and 1373, as well as the 2001 and 2002 EC Regulations, follows that of the UK, as all UK lists become automatically incorporated in the IOM freezing regime. Although the bulk of the international criteria are covered, the system needs to be completed with adequate measures, most importantly in the area of protection of the basic interests and rights of persons affected by the listings.

9. The Financial Crime Unit (FCU), in acting as the FIU, is performing its role adequately and receives a reasonable flow of suspicious transaction reports (STRs). It is a joint police/customs unit supported by civilian personnel and its specific remit as a receiving and processing agency for ML and FT-related disclosures is formalized in the AML Code 2008. Within the FCU, there is a clear separation between the intelligence and the investigative side of the handling of the reports. However, the low number of STRs that result in domestic investigations, and ultimately in a prosecution, raises an effectiveness issue that needs to be addressed, though this is in part explained by the cross-border nature of many of the reported suspicions. Additional resources are being provided to the FCU.

10. The IOM has recently formally adopted a risk-based approach to the application of AML/CFT measures, following the enactment of the FSA 2008. Licenseholders are required to conduct a risk assessment of their businesses and customers and to tailor customer due diligence (CDD) procedures accordingly, with enhanced CDD required where higher risks are identified.

11. With the significant upgrading of requirements, particularly between August and mid-December 2008, the IOM has brought its AML/CFT preventive measures largely into compliance with the FATF Recommendations. Most of the provisions were updated, where necessary, either before or shortly after the assessors' on-site visit, for both financial institutions under FSC

supervision and insurers authorized by the IPA. In many cases (though not all), the assessors were already in a position to observe the level of effectiveness of implementation of the new measures as financial institutions had already introduced them. The recently-enhanced requirements include significant strengthening in areas such as the requirements for business with politically exposed persons (PEPs) and for reliance on non-resident introduced business. Previous potential contradictions between parallel pieces of secondary legislation were also largely eliminated. However, there are instances where the available concessions go beyond a reasonable interpretation of the FATF Recommendations (e.g., some fiduciary deposits). IOM financial institutions are generally well supervised for AML/CFT purposes. The range of available administrative sanctions, while broad, could be enhanced. The quality of implementation of AML/CFT measures in financial institutions appeared generally good, if somewhat variable. The authorities plan additional AML/CFT on-site inspections, particularly for the banking and insurance sectors, to test compliance with the updated requirements.

12. CDD obligations for DNFBPs largely mirror those for financial institutions. TSPs and CSPs conduct substantial cross-border and non face-to-face business and, being considered particularly vulnerable, are closely supervised by the FSC. The on-line gaming sector's entire business, while small, is subject to inherent challenges in relation to CDD. The Department of Home Affairs (DHA), having overall AML/CFT responsibility for the remaining DNFBPs was, at the time of the assessment, seeking to supplement the AML/CFT control structures in place for most lawyers with suitable arrangements for accountants and dealers in precious metals and stones. A firm legal basis for the DHA's role was awaited and implementation of measures for DNFBPs (other than TSPs, CSPs, and most lawyers) were still being developed.

13. The company registration system is well developed and operates within the structures of the FSC. Trusts have long been recognized under IOM law but are not subject to a registration system. The IOM relies on its FSC-licensed TSPs and CSPs to obtain, verify, and retain records of the beneficial ownership and control of legal persons and arrangements and the FSC has devoted considerable resources to improving AML/CFT compliance standards of the CSPs and TSPs.

14. 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, the UK may extend the ratification of any convention to the IOM. The Vienna Convention was extended to the IOM in 1993. However, extension of the Palermo Convention has not yet been requested as IOM law does not yet comply with all its provisions. The UK extended ratification of the UN Convention for the Suppression of the Financing of Terrorism to the IOM in 2008.

15. The range of mutual legal assistance that can be provided by the IOM is broad. MLA requests are frequent and make up a substantial part of the workload of the Attorney General's (AG) Chambers and the FCU and are dealt with constructively and efficiently. Despite the unduly restrictive "designated" countries rule in place at the time of the assessment, there have been no refusals on record since 2004. Overall, the IOM authorities take their responsibilities in the area of international cooperation seriously, including in the FIU (applying Egmont Group principles) and in the financial supervisory area, most notably under the terms of the IOSCO multilateral MOU. Domestic coordination and cooperation is well developed, particularly through the initiatives of the Joint AML Advisory Group, through which all relevant authorities are represented, and through

extensive consultation with the financial institutions and other businesses subject to supervision for AML/CFT purposes.

Legal Systems and Related Institutional Measures

16. The IOM has taken a three strand approach to criminalizing money laundering, differentiating between drug trafficking, terrorism, and other predicate offenses. Through those three offenses, money laundering is criminalized broadly in line with the international standard and many, albeit not all, technical aspects of the Vienna and Palermo Conventions are complied with. All categories of predicate offences listed in the international standard are covered. One shortcoming identified by the assessors is the fact that for the offense of "acquisition, possession or use", IOM law provides for a defense of "giving adequate consideration", regardless of whether or not the perpetrator acted with the knowledge that the property was obtained through the commission of a predicate offense. The defense may potentially be abused by money launderers to avoid criminal liability. Furthermore, the purpose requirements for the various acts constituting money laundering are slightly narrower under IOM law than provided for in the Vienna and Palermo Conventions and the money laundering provision applicable to terrorism-related predicate offenses does not cover all material elements of money laundering provisions of the two Conventions.

17. All three money laundering offenses extend to any type of property that represents the proceeds of crime. Self laundering is criminalized for all acts constituting money laundering except the "acquisition, possession and use". All ancillary offences are criminalized in line with the international standard. The *mens rea* requirement varies depending on the money laundering offences applicable in the specific case. However, at a minimum and with respect to all three money laundering offenses, a person may be held criminally liable if he acted intentionally and with the knowledge that the property involved stems from a criminal source. Based on an English common law principle, intent may be inferred from objective factual circumstances. Criminal liability extends to legal persons.

18. While the statutory sanctions for money laundering are, in the formal sense, comprehensive, dissuasive, and proportionate, the sentences actually imposed by the courts appear rather low. At the time of the on-site visit, the IOM did not have any convictions for autonomous money laundering and the overall number of investigations and prosecutions further supports the conclusion that money laundering is not yet dealt with as a stand-alone offence.

19. While financing of terrorism is criminalized under IOM law, the definition of the offence needs to be amended to fully cover all elements under the International Convention for the Suppression of the Financing of Terrorism. In particular, the definition of "terrorism" should be extended to cover all terrorism offenses as defined in the nine Conventions and Protocols listed in the Annex to the FT Convention. It is unclear whether the terrorism financing offense would extend to situations where the funding of individual terrorist or terrorist organizations related to living or other private expenses. At the time of the on-site visit, there had been no prosecutions or convictions for terrorist financing.

20. The IOM legal framework underpinning the seizure and confiscation system related to proceeds of crime is generally solid and comprehensive. The (similar) relevant provisions of CJA 1990 and DTA 1996 and, since October 22, 2008, POCA 2008 adequately provide for a value-based

confiscation regime capturing any benefit that the offender may have gained as a result of his criminal conduct. The benefit assessment procedure followed by the court is quite detailed and takes into account all factors necessary to come to a fair estimation. The provisions of ATCA 2003 also appropriately focus on the deprivation of the assets related to FT. However, some issues need to be addressed, particularly the low effective asset recovery, the impact of the noted lacunae in the scope of criminalization of ML and FT and that the "corpus delicti" confiscation of the assets laundered is untested and its application doubtful. Equivalent value seizure appears not to be fully covered in all circumstances and the issue identified in the IMF's 2002/03 assessment of nonavailability in the IOM of confiscation of assets of equivalent value in connection with FT remains unresolved.

21. The implementation by the IOM of UNSCRs 1267 and 1373, as well as the 2001 and 2002 EC Regulations, follows that of the UK. All UK lists become automatically incorporated in the IOM freezing regime. The IOM has little or no input in the decisions taken in this context in respect of designations, delisting, and unfreezing. Although this has not yet been used in practice, the IOM has its own listing and freezing provisions in ATCA 2003 Part VII. However, the ATCA 2003 provisions are insufficient to ensure a comprehensive, preventive, pre-investigative approach as required by the international standards. The Orders implementing the relevant UN Resolutions and the EC Regulations, together with the already-existing legal infrastructure, complete the freezing regime to a large extent. However, some issues, mostly of a formal nature, still need to be addressed.

22. The FCU, an active member of the Egmont Group since 2000, acts as the FIU for the IOM. It is a joint police/customs unit supported by civilian personnel. It is operationally independent and its specific remit as a receiving and processing agency for ML and FT-related disclosures by the regulated and associated sector is formalized in the AML Code 2008. The FCU is structured such that its financial intelligence unit operates separately from its investigative law enforcement unit. The statistics spanning the period 2004–2008 show reasonable reporting levels by the financial sector. However, a weakness identified is that the FIU does not have powers of direct or indirect access to financial and other additional information in following up on STRs submitted to it.

23. The number of STRs resulting in an investigation (six in two years) is low and only two prosecutions have been instituted in cases that originated with an STR. While the nature of much of the financial services business conducted in the IOM, involving funds received from abroad on behalf of nonresidents, can make it difficult to prosecute money laundering cases locally and more efficient to transfer cases to other jurisdictions in which the predicate offense may have occurred or the funds or accused persons are located, the assessors consider it important that the IOM seeks also to develop its own case law in this area. This is an effectiveness issue to be addressed for the system as a whole.

24. With regard to the cross-border physical transportation of currency, the IOM opted for a declaration system, in line with the regime in force at the external borders of the EU, which imposes an obligation on persons importing into or exporting from the IOM cash and bearer-negotiable instruments of more than EUR10,000 to make a report to Customs and Excise. However, the controls do not extend to cash transportation by mail between the UK and the IOM.

Preventive Measures—Financial Institutions

25. Coverage of preventive measures in the IOM includes all of the main financial businesses covered by the FATF definition of "financial institution". The main legislative foundation for

customer due diligence (CDD) and other AML/CFT preventive measures in the IOM is the CJA 1990, Section 17 of which defines ML offences, tipping-off offences, and the offence of not reporting suspicious transactions. Section 17F provides the DHA with the power to issue Codes (as secondary legislation) to prevent and detect money laundering, as described in the Act, the open-ended scope of which has been interpreted by the authorities to provide a basis to include FT. As the Codes were subject to a parliamentary approval process, the authorities' interpretation was accepted for purposes of this assessment but the assessors recommended that the opportunity be sought by the authorities to provide a more explicit legal basis in primary legislation. The AML Code 2008 applies to all financial and nonfinancial entities to which the FATF Recommendations relate and includes extensive provisions on CDD largely in line with the international standard.

26. A very significant part of the business covered by the CJA 1990 is within the regulatory ambit of the FSC pursuant to the FSA 2008, which includes among the regulatory objectives of the FSC 'the reduction of financial crime' and under which the FSC issued a Rule Book (as secondary legislation), Part 9 of which provides in detail for CDD for all FSC licenseholders, including CSPs and TSPs. With the updating of the AML Code to mirror most of the provisions of the Rule Book, the previous inconsistencies have been largely eliminated.

27. Insurance business is subject to IPA authorization and supervision. While covered by the AML Code 2008 in the same manner as FSC licenseholders, insurance businesses are also subject to a set of insurance-related AML/CFT requirements, which were updated shortly before this assessment. Much of the insurance legislation was superseded by the Insurance Act 2008 (IA 2008) which came into effect on December 1, 2008, to consolidate most of the previous legislative provisions. The IA 2008 specifies as a regulatory objective of the IPA 'the reduction in...financial crime'. The IPA issued AML/CFT regulations (as secondary legislation) using its powers under the Act and a set of guidance notes which are specified by the Act as binding and, as such, were accepted for purposes of this assessment as other enforceable means.

28. With the significant upgrading of requirements, particularly between August and mid-December 2008, the IOM has brought its AML/CFT preventive measures largely into compliance with the FATF Recommendations, as summarized in the following outline. While anonymous accounts and accounts in fictitious names are not prohibited in primary legislation in the IOM, they are effectively prohibited in secondary legislation, in either a direct or indirect manner. Pursuant to AML Code 2008 paragraph 6, identification procedures apply to new business relationships and include an obligation to identify (and to take reasonable steps to verify) the customer and beneficial owners, in line with the international standard. Appropriate requirements have been introduced in relation to legal persons, parties to legal arrangements, and persons acting on behalf of others. The latest amendments to the Code have also limited the previous scope regarding the timing of the completion of initial CDD. The requirements for the application of CDD to occasional transactions are in line with the FATF Recommendations.

29. The authorities have provided for certain exceptions and concessions in the application of CDD measures, some of which represent an over-generous interpretation of the FATF standard which, in a case where a customer is acting on behalf of another person, expressly calls for a requirement to be in place to take reasonable measures to verify the identity of that other person. In certain limited circumstances, the operation of 'fiduciary deposits' by IOM financial institutions is exempted from such a requirement, which practice the assessors could not reconcile with the FATF

Recommendations. There is also extensive reliance on third parties to conduct all or part of the CDD on behalf of financial institutions. However, the requirements in this regard were strengthened considerably as part of the amendments introduced in the AML Code 2008, bringing them largely into compliance with the international standard.

30. The quality of implementation of AML/CFT measures by financial institutions was found to be mainly of a high standard. In meetings with financial institutions (as well as in some cases their auditors and legal advisors), the assessors found a very high level of awareness of AML/CFT risks and requirements. It was evident that many of the institutions had been closely involved in supporting the development of the latest CDD measures. Most indicated that they apply CDD measures using the permitted risk-based approach. However, it appeared to the assessors that, in some cases, the risk-based approach was being offered as an explanation for less than full compliance with some aspects of the IOM requirements and it is recommended that the regulatory authorities include testing in this regard as part of the on-site visit program. It was not evident to the assessors in all cases that the financial institutions were taking fully into account the increased risk of dealing on such a scale with nonresident non face-to-face business, and the assessors noted an uneven level of controls in practice in some institutions when relying on third parties to have properly conducted CDD measures.

31. With effect from December 18, 2008, AML Code 2008 introduced requirements in line with Recommendation 6 for PEP-related business. The term PEP is defined in detail in AML Code 2008 Paragraph 2 to include an extensive range of nonresident officials and those holding other relevant positions, together with their close relatives and associates. This amendment mirrors the requirements already in place for all entities subject to FSC and IPA-issued requirements, and the assessors found a high level of awareness and compliance by financial institutions with the requirements for PEPs.

32. AML Code 2008 Paragraph 23 introduced a requirement that relevant persons maintain appropriate procedures and controls to prevent the misuse of technological developments, in line with one of the key provisions of Recommendation 8. However, neither the requirements nor the guidance refer to any particular types of technological risks such as internet banking, the use of credit/debit cards as part of account relationships, particularly to nonresidents on a non face-to-face basis; security of computer systems, particularly if customer-accessible, to address the risk of fraud, phishing, or other improper access to customer information. The development of additional guidance was recommended. The assessors welcomed the introduction in the AML Code 2008 of a requirement for adequate measures to compensate for any risk arising as a result of dealing with an applicant for business otherwise than face-to-face.

33. Much of the financial business in the IOM is conducted on a non face-to-face basis for nonresidents. IOM banking, insurance, and other financial services products are marketed globally, including through business introducers. The potentially long distribution chain may increase the exposure of IOM financial institutions to misuse for ML and FT purposes, including through layering and structuring, as they are remote from the customer and face an additional challenge in identifying with confidence the ultimate beneficial owner(s) or controller(s). The IOM authorities have developed a protocol to accommodate the use of business introducers by IOM entities subject to the AML Code 2008. Additionally, they have provided for a defined class of introducer (generally known as ‘Eligible Introducer’), by availing of the provisions of FATF Recommendation 9 in order to eliminate duplication of effort and documentation in cases that meet a set of conditions set out in secondary legislation and developed further in guidance. The assessors found that a range of approaches is

employed by financial institutions in determining whether and, if so, the extent to which they place reliance on the Eligible Introducers to conduct CDD on their behalf—some place full reliance while others are very selective. It is an area on which regulatory authorities should continue to focus particular attention as part of their onsite inspection programs.

34. There are clear requirements in secondary legislation for ongoing due diligence and reporting of suspicious transactions to the FCU, supported by detailed guidance, for their respective supervised institutions, in the FSC's Handbook and the Insurance Guidance Notes (IGN) issued by the IPA. However, the scope of the protection for STR reporting is not sufficient to include all categories of person or circumstances in the international standard and is not limited to good faith reporting. Record keeping requirements have been brought fully into line with the FATF Recommendations. There are no secrecy provisions in legislation to inhibit implementation of AML/CFT requirements, although the assessors recommended the introduction (as planned) of an explicit exclusion from the common law duty of confidentiality to permit financial institutions to exchange information for AML/CFT purposes. Requirements for ongoing due diligence are well developed and comprehensive. However, a more formal approach is needed to support the application of enhanced measures, including countermeasures where warranted, in relation to jurisdictions that do not or inadequately comply with the FATF Recommendations.[5] There are comprehensive requirements, supported by detailed guidance, for the implementation of adequate AML/CFT internal policies, procedures, and controls, with the exception that there is no requirement to maintain an adequately resourced independent audit function dealing with AML/CFT, having due regard to the size and nature of the business.

35. With regard to wire transfers, the IOM opted to implement European Regulation 1781/2006 on Wire Transfers, with appropriate modifications, by means of Orders by the Council of Ministers which constitute secondary legislation. The UK has obtained from EU member states a derogation for the UK to establish agreements with Jersey, Guernsey, and the IOM so that the reduced information requirement can apply to payments passing between the UK and these associated territories (effectively treating them as domestic transfers). Informal funds transfer systems do not appear to be relevant in the IOM context.

36. There is no explicit prohibition on the establishment of a shell bank in the IOM. However, a license issued by the FSC pursuant to FSA 2008 Section 7 is required in order to conduct any activity regulated by that Act and a license may not be issued under Section 7 unless the FSC is satisfied that the applicant is managed and controlled in the IOM. This requirement is developed further in the FSC's General Licensing Policy. For the most part, IOM financial institutions are subject to adequate AML/CFT regulation and supervision, although in some significant areas (banking, insurance) there is a need for additional AML/CFT on-site supervision.

37. In terms of the legal framework, the AML Code 2008, as secondary legislation, is a substantial improvement on the previous AML Code 2007 and moves the IOM much closer to compliance with the detailed provisions of the FATF Recommendations and makes the Code largely consistent with the FSC Rule Book 2008. The Rule Book is supplemented by the substantial guidance

[5] This matter was addressed subsequent to the assessment with the coming into force in July 2009 of the Terrorism (Finance) Act 2009.

contained in the FSC Handbook 2008, which is not regarded as enforceable in its own right. For IPA-regulated insurers, the provisions contained in the IA 2008 and the IAMLR 2008 apply. IAMLR 2008 is supplemented by IGN 2008, which have been accepted as enforceable for purposes of this assessment; however the guidance notes apply only to insurers undertaking long-term insurance business. Regulation and supervision of money-services business in the IOM was transferred with effect from August 1, 2008, from the registration system previously operated by Customs and Excise to the regulation and supervision of the FSC. However, full application by the FSC of AML/CFT measures for money-services businesses did not come into effect until January 1, 2009 and, as such is beyond the scope of this assessment.

38. All IOM financial institutions have a designated regulatory authority for AML/CFT purposes. Statutory fit and proper tests are applied to all license applicants, owners, controllers, directors, and key managers with respect to IOM financial institutions, to ensure their integrity and propriety, in compliance with the international standard. FSC supervision is implemented in accordance with the FSC's published Supervisory Approach (most recently updated in July 2009) which calls for an on-site visit cycle of between one and three years, according to the impact and risk rating of the license holder or group. For banks, the FSC has been conducting risk-assessment focus visits, many of which included AML/CFT-related analysis and file sampling. A round of AML/CFT-themed focus visits is planned for 2009/10 to check compliance with the latest revised requirements. For the IPA, the number of on-site AML/CFT inspections has been limited by resource constraints and additional inspections are envisaged from 2009 onwards.

39. The range of sanctions at the FSC's and IPA's disposal is broad and is complemented by the criminalization of AML/CFT breaches pursuant to the AML Code 2008. Moreover, when serious breaches are identified, the action on the licenseholder would usually be accompanied by 'fit and proper' directions. A limitation that needs to be addressed for the FSC is that it must issue regulations in order to extend the application of its power of financial penalty to new areas, and has yet to do so in the AML/CFT area.

40. While the level of effectiveness of implementation of the AML/CFT requirements is difficult to assess in practice, the assessors found across all financial institutions interviewed a high level of awareness of AML/CFT risks, typologies, and international and IOM requirements. It was clear that many of those interviewed had been closely involved in the recent updating and development of the AML/CFT system.

Preventive Measures—Designated Non-Financial Businesses and Professions

41. CDD obligations for DNFBPs are largely the same as those for financial institutions and are subject to the same strengths and weaknesses. The CSP and TSP sector forms an integral part of the financial services industry of the IOM. It comprises legal professionals and accountants providing both services; all company formation agents; trust service providers who are not legal professionals; and business address and business service providers. The authorities advised that there are approximately 22,000 trusts and 42,000 companies managed or administered in or from the IOM by TSPs and CSPs, respectively. TSPs and CSPs conduct a great deal of cross-border and non face-to-face business and should, therefore, be considered particularly vulnerable from an AML/CFT perspective. However, TSPs and CSPs are authorized and actively supervised by the FSC, with particular focus on AML/CFT compliance.

42. The on-line gaming sector's entire business is subject to inherent challenges in relation to CDD as all business is conducted on a non face-to-face basis, with identification and verification via electronic means. The IOM has authorized one terrestrial casino and 11 on-line casinos, offering a variety of gambling options. The casinos are licensed and supervised by the Gambling Supervision Commission (GSC).

43. The legal profession in the IOM consists of advocates (licensed to practice law) and registered legal practitioners (persons registered in a number of prescribed jurisdictions). Both advocates and legal practitioners are subject to the obligations set forth in the AML Code 2008 but only the former are under the ambit of the IOM Law Society. The latter are not subject to any supervision with respect to compliance with IOM law, a matter which the authorities indicated they are in the course of addressing. The IOM accounting profession is subject to the provisions of the AML Code 2008 and accountants are registered by the DHA. However, at the time of the assessment, the DHA was still in negotiations with the accountancy bodies to agree a basis for an ongoing AML/CFT compliance program. The assessors recommended that an appropriate arrangement be put in place as quickly as possible. Real Estate Agents and Dealers in precious stones and precious metals are also subject to the provisions of the AML Code 2008. The DHA has also been working to develop appropriate measures for other nonfinancial businesses and the assessors recommended that its program of awareness raising should be continued.

44. Implementation of AML/CFT measures for DNFBPs (other than TSPs, CSPs, and most lawyers) was still being developed at the time of the on-site visit. Overall, the DNFBPs interviewed by the assessors seemed to be well informed about their obligations with respect to CDD and record keeping requirements. The FSC devotes substantial resources with a view to improving AML/CFT compliance of TSPs and CSPs. Some advocates noted that, as they would not necessarily complete all initial CDD measures at the outset of a business relationship, the contracted matters would, in some cases, be completed before CDD was complete and the client would never be fully identified: this weakness needs to be addressed.

Legal Persons and Arrangements & Non-Profit Organizations

45. The IOM has three sets of laws governing legal persons, namely the Companies Act 1931-2004, the Companies Act 2006, and the Limited Liabilities Companies Act 1996. While the first two Acts allow for the incorporation of a wide range of corporate entities, including Companies Limited by Shares, Companies Limited by Guarantee, Companies Limited by Guarantee and having a Share Capital, Unlimited Companies, and Protected Cell Companies, the latter provides for and regulates the incorporation of Limited Liability Companies. Trusts have been recognized under IOM law for many years and the trust concept is well established. The Trustee Act 1961 and its subsequent amendments are the main pieces of legislation governing such legal arrangements. In addition, the common law principles of trust law and equity are applied and recognized by the courts in the IOM insofar as they are not contrary to statutory law or local precedent. As of June 30, 2008, about 31,000 companies and close to 23,000 trusts were set up under IOM law.

46. The IOM primarily relies on its licensed CSPs and TSPs to obtain, verify, and retain records of the beneficial ownership and control of legal persons. All IOM legal entities that are incorporated under the Companies Act 2006 must utilize the services of and provide the Companies Registry with the name and address of the respective corporate service provider. Companies incorporated under the

Companies Act 1931-2004, the Limited Liabilities Companies Act 1996 as well as legal arrangements are not required to utilize licensed CSPs and TSPs but may choose to do so. It is estimated that 70 percent of all companies registered in the IOM utilize the services of licensed CSP. The number of trusts administered by licensed TSP is unknown. Although the Companies Registry maintains and administers some information regarding the management and administration of companies, its main role with respect to beneficial ownership information is to link an entity with a specific IOM CSP and thus allow the competent authorities to locate beneficial ownership information. Trusts are not registered in the IOM.

47. CSPs and TSPs are obliged to identify in all cases the natural person who ultimately owns or controls a customer or a person on whose behalf a transaction is being conducted as well as any person who exercises ultimate effective control over a legal person, and to take reasonable steps to verify the identity of those persons based on reliable information. For those companies or legal arrangements not utilizing the services of licensed CSPs and TSPs, no formal measures are in place to ensure that beneficial ownership information is obtained, verified, and maintained. Persons providing director services, nominee shareholders, protectors/enforcers, and letters of wishes are permitted and frequently used for trusts under IOM law.

48. IOM charitable bodies are registered with the General Registry, which has undertaken a desk-top review of registered charities' objectives and mandates. Although no vulnerabilities to abuse for FT purposes were identified, the assessors recommended that the authorities proceed with their planned review of the sector.

National and International Co-operation

49. Cooperation and coordination between the domestic authorities is well organized and effective, particularly through the initiatives of the Joint AML Advisory Group, through which all relevant authorities are represented, and through extensive consultation with the financial institutions and other businesses subject to supervision for AML/CFT purposes.

50. The IOM is a British Crown Dependency and as such is not empowered to sign or ratify international conventions on its own behalf. Rather, the UK is responsible for the IOM's international affairs and, following a request by the IOM Government, may extend the ratification of any convention to the IOM. As a general principle, the IOM seeks to have extended to it all conventions ratified by the UK. However, such extension is only requested after IOM legislation has been determined to be in compliance with any given convention. Whereas the UK's ratification of the Vienna Convention has been extended to the IOM on December 2, 1993, extension of the Palermo Convention has not yet been requested as IOM law does not yet comply with all its provisions. The UK has extended ratification of the UN Convention for the Suppression of the Financing of Terrorism to the IOM on September 25, 2008. Additionally, ten out of the other 15 international conventions and protocols relating to the fight against terrorism have been extended. However, not all of the convention's provisions have been implemented.

51. There is no overarching legislation regulating the mutual legal assistance (MLA) practice of the IOM. In providing such assistance, the judicial authorities use the domestic provisions contained in the CJA 1990, CJA 1991, DTA 1996, and ATCA 2003, as appropriate. Most provisions apply to criminal activity both in and outside the IOM and the range of mutual legal assistance that can be

provided according to the relevant Acts is quite broad and include the following measures: collection, production, search, and seizure of information and documents. The fact that the MLA request may contain fiscal aspects, both formally and in practice, does not constitute grounds for refusal.

52. The legal framework for extradition is comprehensive and compliant with the international standards. In the absence of precedents, only the formal provisions can be assessed.

53. Providing international cooperation to foreign counterparts is a very important part of the FIU assignment in an offshore jurisdiction like the IOM. The FCU/FIU is quite active in the Egmont network of FIUs. Although not required, in some instances the cooperation is underpinned by bilateral MOUs. Information requests from a counterpart FIU are complied with to the greatest extent within the boundary of use for intelligence purposes. The FIU to FIU cooperation is governed by the Egmont principles of information exchange. Besides direct bilateral contacts, the police use the international communication network of Interpol. Assistance to other police authorities is routinely granted, as long as it does not involve coercive measures. Customs and Excise 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.

54. Both the FSC and IPA are empowered (under the FSA 2008 and Insurance Act 2008, respectively) to enter into MOUs. The FSC has entered into a range of MOUs and is a full signatory to the IOSCO Multilateral Memorandum of Understanding (MMOU). The IPA is a signatory to a number of MOUs. Both the FSC and IPA are empowered to provide information to supervisory counterparts both spontaneously and on request. The scope of the powers includes all relevant information held by the supervisory authorities. There are no secrecy provisions in the IOM that would restrict the capacity of the supervisory authorities to share confidential information with foreign counterparts, where warranted and appropriate.

55. Detailed statistics on international requests for intelligence/assistance are kept by the FCU, including the number of spontaneous referrals. No distinction is made in the statistics, however, between police and FIU originated requests. It would give a clearer picture if the statistics would reflect that distinction. Statistics for various forms of international cooperation are also maintained by the supervisory authorities. Many of the information exchanges arise under the IOSCO MMOU, including those related to insider dealing. Information requests in conducting ‘Fit and proper’ tests represent another common application of international cooperation.

Other Issues

56. While the relevant authorities are generally well resourced, the regulatory authorities would benefit from additional resources to sustain an appropriate level of AML/CFT onsite inspection work, particularly for banks and insurance businesses. Some additional resources are also needed by the GSC and DHA to carry out their respective AML/CFT responsibilities. The authorities have approved additional resources for the FCU.

57. Relevant statistics are well maintained in most areas, including by the regulatory authorities. However, comprehensive statistics are not maintained on seizures and confiscations.

1. GENERAL

1.1. General Information on the Isle of Man

58. Located in the middle of the Irish Sea, the Isle of Man (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 just over 80,000 (2006 interim census). There are no immigration barriers between the IOM and the United Kingdom (UK) or Ireland, but there is a work permit system that controls the right to take up employment. The local currency is the Manx pound, which is on a par with the British pound (GBP). There are no exchange controls.

59. 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. The IOM has never been part of the UK nor the European Union (EU) and receives no funding from either. It is not represented in the British parliament nor in Brussels. However, The IOM has a limited relationship with the EU as set out in Protocol 3 to the UK's Act of Accession annexed to the Treaty of Accession by which the UK acceded to the Treaty of Rome in 1972, allowing for free trade in agricultural and manufactured products between the IOM and EU members. Apart from matters relating to this special relationship, which includes customs, the IOM is not bound by EU legislation. The IOM chose to become part of the EU's VAT regime.

60. 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 nine 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.

61. In 2005/6, the IOM's Gross Domestic Product (GDP) was GBP1.6 billion. Over the past ten years, the IOM's average real annual rate of economic growth has been 7.8 percent, continuing some quarter of a century of unbroken growth. Financial services is the single largest component of GDP, accounting for 36 percent. The IOM has a working population of around 43,000 and a current unemployment rate of 1.3 percent.

62. The IOM has its own legal system and jurisprudence. English law is not directly of application in general, but the IOM legal system is based on the principles of English common law which are shared by many Commonwealth countries. IOM law is accordingly very similar to English law in areas such as crime, contract, tort, and family law. However, in certain areas, although modeled on English law, IOM law has adapted to meet the IOM's own special circumstances, particularly with regard to direct taxation, company law, and financial supervision. The IOM's High Court judges hold the ancient office of Deemster and have jurisdiction over all criminal and civil matters. Advocates at the IOM Bar have the fused rights of solicitors and barristers. The rarely-exercised final right of appeal to the Judicial Committee of the Privy Council remains. The IOM has fully incorporated into its law the basic rights set out in the European Convention on Human Rights through its Human Rights Act 2001.

63. No particular structural issues were identified in the course of the assessment that could give rise to an increase vulnerability to abuse of the system for ML or FT purposes. Standards of governance and transparency appear to be high. In the area of anti-corruption, the IOM has enacted a revised Corruption Act in July 2008 to bring IOM legislation largely into compliance with the UN Convention against Corruption, but a number of ancillary legislative provisions need to be adopted and were being progressed at the time of the assessment so that the UK's ratification of the convention can be extended to the IOM. The court system appears to be efficient and all indications point to high ethical and professional standards across the public sector. The assessors can confirm that they found a significant improvement in the overall culture of compliance across the financial sector by comparison with the more accommodating pre-2003 approach, as acknowledged by some of the financial sector participants. Most legal and accounting professionals are members of professional bodies which carry out monitoring procedures for quality control and legal compliance and, as detailed in this report, progress is currently being made regarding the implementation of AML/CFT measures by lawyers and accountants.

1.2. General Situation of Money Laundering and Financing of Terrorism

64. The IOM is, in general, a low-crime environment, though the authorities have a continuing concern regarding the increasing incidence of drug-related crimes. As discussed in detail in this assessment, the nature of the financial sector business conducted in or from the IOM creates a material vulnerability to being used in the layering and integration stages of money laundering schemes. As acknowledged by the IOM authorities, some characteristics of the IOM financial system point to an increased risk of abuse for ML or FT purposes. While in reality not all of this business is high-risk, much of it would fall within the range of categories suggested by the FATF Methodology as examples of higher-risk business, including as follows:

- The authorities indicated that more than 90 percent of the customer relationships and of financial service business conducted are on a non face-to-face basis for nonresidents of the IOM[6];
- In many cases the business relationship is established through introducers (IOM or foreign) that are subject to varying levels of regulation, depending on their origin. Subject to certain controls, IOM financial institutions are permitted to rely on the introducers to conduct CDD on their behalf;
- Financial services provided include private banking facilities for non-residents; and
- The use of legal persons and arrangements such as trusts is prevalent, both as asset-holding vehicles and as part of more complex structures that have the potential to create an additional challenge for IOM financial institutions in meeting their

[6] While deposit statistics indicate that approximately 30 percent of bank deposits in the IOM are from resident sources, much of this business relates to deposits placed with banks by IOM fiduciaries which are acting on behalf of nonresident beneficial owners.

requirement to identify accurately the customer and the ultimate beneficial owner or controller.

65. This environment, designed by the authorities to attract financial services business and employment to the IOM, brings with it a material risk of financial crime, typically emanating from other jurisdictions and seeking to avail of the financial services available in the IOM. This assessment will consider carefully whether and to what extent the preventive measures put in place in the IOM are adequate to measure, manage, and mitigate the resulting risk. Emphasis will also be placed on assessing the willingness of the IOM authorities to cooperate with their international counterparts in addressing cross-border financial crime, and in assessing the effectiveness of the measures in place.

66. There have been no convictions or prosecutions for terrorist financing in the IOM; neither have there been any terrorist incidents.

1.3. Overview of the Financial Sector

67. Banking and insurance services represent the most significant financial service businesses in the IOM. The authorities provided the following analysis of the financial sector as at end-March 2008. At that date, there were 43 deposit takers[7], together with a range of other financial institutions, as follows:

- 40 licensed banks (as at 31 March 2008) of which only two are locally-based. The remainder are either branches or locally incorporated subsidiaries of banking groups headquartered elsewhere, predominantly in the UK or Ireland. Three banks are part of South African groups (two groups) and another is Swiss-owned. Most banks rely on their group for treasury functions and mainly provide client services to corporate and personal clients. As well as taking deposits, banks are also permitted to undertake a normal range of banking services such as lending, money transfers and currency exchange. The deposit base (net of local inter-bank placings) totaled GBP52.36 billion as at March 31, 2008; and

- Three branches of UK building societies.

- There were, in practice, three licensed stockbrokers. Two were locally incorporated and the other is a branch of a Guernsey firm (which also has a branch in Jersey) which is ultimately UK-owned.

- 23 firms provided asset management services to collective investment schemes and portfolio management for other customers.

- 26 firms provided management and administration services to collective investment schemes.

- There were 38 financial advisers. These were mainly small businesses, which provided a limited range of services, predominantly for private clients.

[7] One of these banks went into provisional liquidation in October 2008 and its license was suspended.

- As shown in the table below, there were 30 life insurers, 157 nonlife insurers, 23 insurance managers, 33 general insurance intermediaries, and 86 administrators of retirement benefits schemes–an expanding business line for the IOM.

Statistical Table 1. Structure of Financial Sector

Type	Activity (per Ref below)	No.	Domestic Branches	Overseas branch	Size	Authorized by	Supervisor	AML /CFT oversight
Deposit takers	1,2,3,4,5 6, 10, 13	43	62	4	£52bn deposits	FSC	FSC	FSC
Investment Business – Stockbrokers	7(a) to (d), 10, 11	3	3	Nil		FSC	FSC	FSC
Investment Business –asset managers for collective investment schemes and portfolio managers	7(a to d), 10, 11	23	23	Nil		FSC	FSC	FSC
Investment Business – Financial Advisers	11	38	38	Nil		FSC	FSC	FSC
Services to Collective Investment Schemes – manager and administrator	10, 11	26	26	Nil	$53bn funds	FSC	FSC	FSC
Money Service Businesses	4,5, 13	21	21			FSC	FSC	FSC
Money Lenders	2	51				IOMOFT		
Life Insurers	12	30	17	13	£37.69bn	IPA	IPA	IPA
Non-Life Insurers	12	157	151	6	£5.20bn	IPA	IPA	IPA
Insurance Managers	12	23	23	Nil	N/A	IPA	IPA	IPA
General Insurance Intermediaries	12	33	33	Nil	N/A	IPA	IPA	IPA
Retirement Benefits Schemes Administrators	12	86	86	Nil	N/A	IPA	IPA	IPA

68. The following table sets out the types of financial institutions that can engage in the financial activities that are within the definition of "financial institutions" in the FATF 40+9.

Statistical Table 2. Financial Activity by Type of Financial Institution

Ref	Financial Institution Definition from FATF Methodology	Institution Type	Authorized / Licensed Activity
1	Acceptance of deposits and other repayable funds from the public. (This also captures private banking)	Bank/Deposit taker	**Licensed under section 7 of the Financial Services Act 2008 to carry on regulated activities falling within Class 1 of the Regulated Activities Order 2008.**
2	Lending (This includes inter alia: consumer credit; mortgage credit; factoring, with or without recourse; and finance of commercial transactions (including forfeiting).)	Bank/deposit taker, Building Society, Money Lender	Licensed under section 7 of the Financial Services Act 2008 to carry on regulated activities falling within Class 1 of the Regulated Activities Order 2008. Under section 1(1) of the Moneylenders Act 1991, the Isle of Man Office of Fair Trading shall maintain a register of persons carrying on the business of lending money.
3	Financial Leasing (This does not extend to financial leasing arrangements in relation to consumer products.)	Bank/deposit taker	Licensed under section 7 of the Financial Services Act 2008 to carry on regulated activities falling within Class 1 of the Regulated Activities Order 2008.
4	The transfer of money or value. (This applies to financial activity in both the formal or informal sector *e.g.* alternative remittance activity. See the Interpretative Note to Special Recommendation VI. It does not apply to any natural or legal person that provides financial institutions solely with message or other support systems for transmitting funds. See the Interpretative Note to Special Recommendation VII.)	Money Service Business Bank/deposit taker	Licensed under section 7 of the Financial Services Act 2008 to carry on regulated activities falling within Class 1 (deposit taking) or Class 6 (money transmission services) of the Regulated Activities Order 2008.
5	Issuing and managing means of payment (e.g. credit and debit cards, checks, traveler's checks, money orders and bankers' drafts, electronic money).	Money Service Business Bank/deposit taker	Licensed under section 7 of the Financial Services Act 2008 to carry on regulated activities falling within Class 1 (deposit taking) or Class 6 (money transmission services) of the Regulated Activities Order 2008.
6	Financial guarantees and commitments.	Bank/deposit taker	Licensed under section 7 of the Financial Services Act 2008 to carry on regulated activities falling within Class 1 of the Regulated Activities Order 2008.

Ref	Financial Institution Definition from FATF Methodology	Institution Type	Authorized / Licensed Activity
7(a-d)	Trading in: (a) Money market instruments (checks, bills, CDs, derivatives etc.). (b) Foreign exchange. (c) Exchange, interest rate and index instruments. (d) Transferable securities.	Investment Business – Stockbroker - asset managers for collective investment schemes and portfolio managers Bank/ deposit taker re FX transactions etc	Licensed under section 7 of the Financial Services Act 2008 to carry on regulated activities falling within Class 2 (investment business) or Class 3 (services to Collective Investment Schemes) of the Regulated Activities Order 2008 as appropriate. Licensed under section 7 of the Financial Services Act 2008 to carry on regulated activities falling within Class 1 of the Regulated Activities Order 2008.
7(e)	Trading in: (e) Commodity futures trading.		Licensed under section 7 of the Financial Services Act 2008 to carry on regulated activities falling within Class 2 (investment business) of the Regulated Activities Order 2008.
8	Participation in securities issues and the provision of financial services related to such issues.		Licensed under section 7 of the Financial Services Act 2008 to carry on regulated activities falling within Class 2 (investment business) of the Regulated Activities Order 2008.
9	Individual and collective portfolio management.		Licensed under section 7 of the Financial Services Act 2008 to carry on regulated activities falling within Class 2 (investment business) of the Regulated Activities Order 2008.
10	Safekeeping and administration of cash or liquid securities on behalf of other persons.	Bank/deposit taker Investment Business – Stockbroker - asset managers for collective investment schemes - Services to Collective Investment Schemes – Manager and administrator, custodian and trustee.	Licensed under section 7 of the Financial Services Act 2008 to carry on regulated activities falling within Class 1 (deposit taking), Class 2 (investment business) or Class 3 (services to Collective Investment Schemes) of the Regulated Activities Order 2008 as appropriate.

Ref	Financial Institution Definition from FATF Methodology	Institution Type	Authorized / Licensed Activity
11	Otherwise investing, administering or managing funds or money on behalf of other persons	Retirement Benefits Schemes Administrators Investment Business – Stockbroker - Asset managers for collective investment schemes and portfolio managers - Financial Advisers - Services to Collective Investment Schemes – Manager and administrator	Registered in accordance with section 36 of the Retirement Benefits Schemes Act 2000 acting by way of business as a pension scheme administrator. Licensed under section 7 of the Financial Services Act 2008 to carry on regulated activities falling within Class 2 (investment business) or Class 3 (services to Collective Investment Schemes) of the Regulated Activities Order 2008.
12	Underwriting and placement of life insurance and other investment related insurance. (This applies both to insurance undertakings and to insurance intermediaries (agents and brokers).	Life Insurers Non-Life Insurers (including captive insurers and re-insurers) Insurance Managers	Authorized under Section 8 of the Insurance Act 2008[8] to carry on the business of insurance (linked and non-linked long term business of Class 1 and Class 2 or Class 10 (reinsurance of such business only) respectively as set out in Regulation 2(2) of the Insurance Regulations 1986). Authorized under Section 8 of the Insurance Act 2008 to carry on general insurance business of Classes 3 to 9 and 11 and 12 as set out in Regulation 2(2) of the Insurance Regulations 1986. Namely: • Marine, aviation & transport • Property • Motor • Pecuniary loss • Liability • Credit & suretyship • Personal miscellaneous • Reinsurance of such business • Restricted (captive) business Registered in accordance with Section 23 of the Insurance Act 2008 providing management services for one or more insurers.

[8] The Insurance Act 2008 came into force on December 1, 2008 and superseded the Insurance Act 1986 (as amended) which contained the same licensing provisions.

Ref	Financial Institution Definition from FATF Methodology	Institution Type	Authorized / Licensed Activity
		General Insurance Intermediaries	Registered in accordance with Section 24 of the Insurance Act 2008 acting as a general business intermediary as defined in Section 54 of that Act.
	Otherwise investing, administering or managing funds or money on behalf of other persons.	Retirement Benefits Schemes Administrators	Registered in accordance with Section 36 of the Retirement Benefits Schemes Act 2000 acting by way of business as a pension scheme administrator.
13	Money and currency changing.	Money Service Business Bank/deposit taker	Licensed under section 7 of the Financial Services Act 2008 to carry on regulated activities falling within Class 1 (deposit taking) or Class 6 (money transmission services) of the Regulated Activities Order 2008.

1.4. Overview of the DNFBP Sector

Table of information regarding Designated Non-Financial Businesses and Professions

Type	No.	Domestic Branches	Oversea s branch	Size	Authorized by:	Supervisor	AML /CFT oversight
1. Casinos (including internet casinos)	1	1	0		GSC	GSC	GSC
2. Real estate agents	20	28	2		DOLGE	DHA	DHA
3. Lawyers, notaries,	Isle of Man Law Society.						
4. Accountants	89	91	Nil		DHA	DHA	DHA
5. Trust Service Providers	120	120	Nil	22,000 trusts	FSC	FSC	FSC
6. Corporate Service Providers	185	185	Nil	42,000 companies	FSC	FSC	FSC

69. The Gambling Supervision Commission (GSC) licenses one terrestrial casino which operates within premises in the IOM. Under the Online Gambling Regulation Act 2001 (OGRA), the GSC also licenses other gambling websites, although none of these are strictly online casinos; instead offering a variety of gambling types, including sports book betting, peer-to-peer betting, poker and other card games. As at June 30, 2008, the GSC licensed ten such companies, with a further three companies awaiting licenses.

70. Dealers in precious metals and precious stones are covered as relevant businesses at Paragraph 24 of Schedule 1 of the Criminal Justice (Money Laundering) Code 2008. This refers to "the business of dealing in goods of any description (including dealing as an auctioneer) whenever a transaction involves accepting a total cash payment of EUR15,000 or more". Responsibility for their oversight rests with the Department of Home Affairs (DHA).

71. The FSC has authorized and supervised Corporate Service Providers (CSPs) since 2001 and Trust Service Providers (TSPs) since 2005. As at 31 March 31, 2008 there were 185 licensed CSPs and 120 licensed TSPs. Almost all of the TSP licenseholders are either CSP licenseholders in their own right or are part of a group which also contains a CSP licenseholder.

1.5. Overview of commercial laws and mechanisms governing legal persons and arrangements

72. The IOM has three sets of laws governing legal persons, namely the Companies Act 1931-2004, the Companies Act 2006, and the Limited Liabilities Companies Act 1996. While the first two Acts allow for the incorporation of a wide range of corporate entities, including Companies Limited by Shares, Companies Limited by Guarantee, Companies Limited by Guarantee and having a Share Capital, Unlimited Companies, and Protected Cell Companies, the latter provides for and regulates the incorporation of Limited Liability Companies.

73. Both the Companies Act 1931-2004 and the Companies Act 2006 provide for exactly the same types of corporate forms. However, the registration and management requirements for the two acts differ considerably. In particular, all legal persons incorporated pursuant to the Companies Act 2006 (2006 Companies) have to have a registered agent licensed pursuant to the FSA 2008. While no such registered agent requirement exists for legal persons incorporated pursuant to the Companies Act 1931–2004 (1931 Companies), the amount of information to be filed with the Companies Registry upon incorporation is much more comprehensive than for 2006 Companies. It is at the discretion of the company founder to choose under which act any company form is to be incorporated.

74. The Companies Act 2006 was introduced to respond to the desire of the private sector (in particular the corporate service providers) to have available a more flexible and modern company structure with less stringent registration requirements. The Companies Act 1931–2004 structure remains available not least so that local businesses and sole traders can incorporate without having to incur the costs of a professional corporate service provider.

75. Overall, the IOM relies on its licensed corporate service providers to obtain, verify, and retain beneficial ownership information on legal entities. The FSC is granted a wide range of powers to access any information and documentation held by licenseholders, including corporate service providers. Although the Companies Registry maintains a certain amount of information regarding the management and administration of companies, it does not collect and maintain information on the beneficial owners of registered companies. However, the Companies Registry can still serve a useful role in that respect by making it possible to link many of the registered legal entities with a specific IOM corporate service provider and thus allow the competent authorities to locate beneficial ownership information.

76. All company forms obtain full legal capacity upon registration with the Companies Registry, which is maintained and administered by the FSC. All information and documentation contained in the Companies Registry is accessible by the public. Since 2004 all information and documentation held at the registry is also available in electronic form, including online.

Companies Act 1931-2004

77. For 1931 Companies, registration typically requires the filing of information on the registered office, the company directors, secretaries and shareholders, and of a copy of the memorandum and articles of association. The memorandum of association must state the name of the company, whether the company is a public or private company and that, in respect of a company limited by shares or by guarantee, the members have limited liability and in the case of a company limited by guarantee, each member undertakes to contribute a prescribed sum to the company in the event of its being insolvent upon liquidation. In the case of a company having a share capital, the amount and division of such share capital.

78. In addition, the Companies Registry has to be provided with a statement containing the address of the registered office of the company, which must be in the IOM, the names, address, nationality, and business occupation of the company's directors and secretary. It is expressly required that the person delivering the information to the FSC has to be an IOM resident. In the absence of such a statement the Registrar will not incorporate the company.

79. 1931 Companies require at least one shareholder and two directors. Section 9 Companies Act 1974 expressly prohibits the use of legal persons as company directors. All companies have to file an annual return with the Companies Registry containing, at a minimum, the address of the registered office, the names and addresses of all shareholders, directors and the secretary, as well as the number of shares held by each shareholder.

Companies Act 2006

80. In comparison, registration of 2006 Companies merely requires that the Companies Registry is provided with the memorandum of association which has to contain, amongst other things, the name of the company, the type of company founded, the name of the first registered agent as well as the address of the first registered office, and the full name and address of each first subscriber. Pursuant to Section 73 of the Companies Act 2006 the registered office has to be a physical address in the IOM and Section 74 requires that the registered agent is licensed by the FSC.

81. 2006 Companies require at least one shareholder and one director. Section 91 (4) Companies Act 2006 allows for the use of legal persons as company directors provided that the corporate director holds a license issued by the FSC. While 2006 Companies are required to maintain shareholder and director registers at the office of the registered agent in the IOM, the filing of those registers in the Companies Registry is optional.

82. All 2006 Companies have to file an annual return with the Companies Registry containing, at a minimum, the updated name and address of the licensed registered agent.

83. Both Companies Acts allow for the issuance of nominal shares by companies limited by shares, companies limited by shares and a guarantee, or unlimited companies with shares. However, the issuance of new bearer shares is not allowed and rights and obligations attached to existing ones issued under the 1931 Companies Act may only be exercised after registration with the shareholder register maintained at the registered office.

Limited Liability Companies Act

84. To incorporate a Limited Liability Company ("LLC"), it is necessary to file with the Companies Registry the articles of organization, a consent form signed by the registered agent named in the articles of organization, as well as a statement of the registered office in the IOM. Section 7 of the Limited Liabilities Companies Act requires that the articles of organization contain the company name, the names and addresses of all company members, and the name and address of the registered agent in the IOM. LLCs are required to file annual returns with the Companies Registry, containing the updated address of the registered office, and the name and address of the registered agent and of the managers and members of the companies.

Trusts

85. Trusts have been recognized under IOM law for many years and the trust concept is well established in the island. The Trustee Act 1961 and its subsequent amendments are the main pieces of legislation governing such legal arrangements. In addition, the common law principles of trust law and equity are applied and recognized by the courts in the IOM insofar as they are not contrary to statutory law or local precedent. Express trusts, implied trusts, resulting trusts as well as constructive trusts are all recognized and utilized in the IOM. Since 1996 IOM law also allows for the enforcement of purpose trusts provided that the trust purpose is certain, reasonably enforceable, and not contrary to the law. IOM also allows for the setting up of private trust companies (PTC), which typically act as trustee for one or more family trusts only and are exempted from the licensing requirements under the FSA. Trusts with a PTC as trustee have to be administered by a natural or legal person holding a Trust Service Provider (TSP) license issued by the FSC.

86. IOM trusts are generally set up by way of deed, declaration, or will. It is allowed under IOM law for the settlor to be the beneficiary, including the sole beneficiary, of a trust and "trustee" is defined by the Trustee Act 1961 to include trustees with a beneficial interest in the trust property. In some cases, however, IOM courts have decided to strike down so-called "sham trusts", where the settler controlled the trustee to the extent that the trustee could no longer be considered to be acting independently of the settlor. Protectors and enforcers are allowed under IOM law and are used by some trust service providers. IOM law permits the redomiciliation of trusts to the law of other jurisdictions but any attempt to delay or frustrate a criminal investigation would represent an offense under the CJA 1990 and the DTA 1996, respectively, on the part of the trustee. It does not appear that forced redomiciliations or 'flee' clauses are in general use in the IOM. The Convention on the Law Applicable to Trusts and on their Recognition has been extended to the IOM and IOM law recognizes foreign trusts through the Recognition of Trusts Act 1988.

87. Other than for charitable trusts, IOM law does not impose a registration requirement for trusts and there is no general filing requirement for trust accounts or other trust information.

88. As of end–June 2008, 31,711 companies were incorporated under IOM law, of which 28,323 were 1931 Companies, 2,850 were 2006 Companies and 538 were LLCs. While the number of incorporations of 1931 Companies seems to be declining, the growth in the number of 2006 Companies has leveled off. Of the 31,711 companies incorporated under IOM law, 23,259 are under administration by corporate service providers licensed by the FSC.

89. As of December 2007, 22,785 trusts, including private trusts, were administered by trust service providers licensed by the FSC. The statistics are based on the information filed by licensed trust service providers through the annual return. As the licensing requirement was only implemented in 2005, there are no statistics for the previous years that would show whether or not the number of administered IOM trusts is increasing.

Companies and Trust Registered in the IOM						
End-December:	**2003**	**2004**	**2005**	**2006**	**2007**	**June 30, 2008**
1931 Act Companies	33,351	32,726	30,847	30,870	30,380	28,323
2006 Act Companies				254	2,098	2,850
LLCs	72	51	51	39	58	47
TOTAL REGISTERED	**33,423**	**32,777**	**30,898**	**31,163**	**32,536**	**31,220**
Administered Trusts						22,785

1.6. Overview of strategy to prevent money laundering and terrorist financing

AML/CFT Strategies and Priorities

90. While the IOM government has not published an AML/CFT strategy, as such, a political commitment has been given by the IOM authorities, in correspondence with the FATF and in public statements, to adhere to the principles of the FATF Recommendations. The authorities informed the assessors that the IOM attaches the highest importance to having a robust and enforceable regime for the prevention of money laundering and for countering the financing of terrorism. It is significant that, in addition to the stated objectives of the Financial Crime Unit (FCU) —the IOM financial intelligence unit (FIU)—both of the main supervisory authorities have been assigned legislative objectives related to the reduction in financial crime.

91. The commitment is evidenced also by the level of resources committed by the authorities to updating the AML/CFT legislative framework and providing detailed guidance to support implementation by the financial sector and DNFBPs, particularly in the 18–24 months prior to this assessment.

92. The financial sector has been an active participant in the development of the IOM's AML/CFT strategy. Through their active participation with the authorities in the Joint Anti-Money Laundering Advisory Group, they have ensured that AML/CFT measures introduced reflect commercial reality and, where relevant, are largely consistent with those already required of their financial sector parent companies, particularly in the UK.

93. The IOM authorities participate in Crown Dependency meetings with their counterparts from Jersey and Guernsey in respect of AML/CFT issues. These occasions greatly assist in being able to mount a coordinated fight against any economic crime which may affect the Crown Dependencies.

The Institutional Framework for Combating Money Laundering and Terrorist Financing

Department of Home Affairs

94. The core function of the Department of Home Affairs is to ensure community safety. The Department's overall responsibilities include, inter alia, the police service (within which is located the FIU) and the prison service. The DHA has a statutory role in issuing AML Codes under the Criminal Justice Act 1990 (CJA 1990). It is also the default authority developing appropriate AML/CFT measures for those DNFBPs and other nonfinancial businesses that do not come under the supervision of one of the other authorities described below.

95. The Department has set up a regulatory mechanism for dealing with other relevant businesses and is in an advanced stage of putting in place the necessary codes and rules to specifically regulate accountants, estate agents, lawyers, motor dealers, auctioneers, jewelers and dealers in other high value goods.

The Treasury

96. Among the range of functions carried out by the Treasury, a number impact on AML/CFT. For example, Customs and Excise is a division of the Treasury. Also, it is the Treasury Minister who introduces to the IOM parliament, Tynwald, secondary legislation on AML/CFT being proposed by the regulatory authorities. The Treasury is represented on the Joint Anti-Money Laundering Advisory Group (JAMLAG) by officials from both the Customs and Excise Division and from the Corporate Strategy Division. The Treasury and the FSC have a Memorandum of Understanding (MOU) in place governing the respective responsibilities of the two bodies. MOUs are being progressed with the IPA and the GSC.

Customs and Excise

97. The Customs and Excise Division of Treasury has an important role to play in AML/CFT, including by way of border controls and, in particular, implementing measures for cross-border movement of cash or negotiable instruments. The Criminal Justice Act 1990 and Drug Trafficking Act 1996 (and their replacement in the Proceeds of Crime Act 2008) provide powers for customs officers in combating money laundering. Customs officers form part of the staffing of the Financial Crime Unit. A relevant provision of POCA 2008 was brought into force from October 22, 2008 thereby inserting a new Section 77A into the PPPA 1998 that provides that customs officers at the FCU, when authorized in writing by the AG, shall have the powers of a constable in relation to their work at the FCU. The AG signed the necessary authority on November 11, 2008 for officers working at, or available to work at, the FCU to have the powers of a police constable.

Chief Secretary's Office

98. The Chief Secretary's Office has various functions including providing leadership of the Civil Service and to facilitate greater cross Departmental working. It also leads the public service's response to the Council of Ministers' initiative on delivering Corporate Governance and Business Planning across Government. It provides impartial advice to the Chief Minister and to the Council of Ministers, particularly as regards the implications of proposed changes in policy or legislation, or in external developments. It promotes and continues the evolution of the constitutional relationship

between the Isle of Man and the United Kingdom and ensures recognition of the Island's interests internationally whilst honoring its international obligations.

99. The Chief Secretary's Office also has functions with regard to the Lieutenant Governor that include providing advice and assistance in the exercise of his Crown responsibilities. Important among these responsibilities is the process of obtaining Royal Assent for all new legislation to be adopted in the IOM. The Chief Secretary's Office also liaises directly with the UK administration regarding international matters, including the extension to the IOM of international conventions.

Attorney General's Chambers

100. The Attorney General for the Isle of Man is appointed by Her Majesty the Queen and holds office during Her Majesty's pleasure. He is ex officio a member of the Legislative Council and attends meetings of the Council of Ministers. HM Attorney General is the legal adviser to the Crown in the Isle of Man and the Government of the Isle of Man. He is also responsible for the prosecution of offenses in the Court of General Gaol Delivery and for the drafting of Government legislation. The Attorney General's Chambers also acts as the competent authority for the receipt of requests for mutual legal assistance in criminal matters from other jurisdictions (including requests from other jurisdictions for the restraint, confiscation, and forfeiture of property in the IOM). The Attorney General's Chambers 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 AG's Chambers is represented at JAMLAG and the Attorney General "chairs" on a rotation basis with the other respective AGs, the inter-Islands' Crown Dependency Meetings which considers AML/CFT issues.

Joint Anti-Money Laundering Advisory Group ("JAMLAG")

101. JAMLAG is the principal forum for discussing AML/CFT issues in the IOM. This is an advisory rather than a policy making group which meets regularly. It comprises regulators, law enforcement authorities and industry and professional representatives. Treasury and the Attorney General's Chambers are also invited to attend. Chairmanship of JAMLAG rotates by meeting between the Chief Executives of the Department of Home Affairs, the Financial Supervision Commission and the Insurance and Pensions Authority. Industry's views on proposed changes to AML/CFT legislation and Regulatory Codes are also sought through the JAMLAG forum.

Criminal justice and operational agencies

Financial Crime Unit (FCU) incorporates the Financial Intelligence Unit (FIU)

102. The FCU is a specialized department within the Constabulary and is headed by a Detective Chief Inspector who is part of the Constabulary's Senior Command Team. The major investigative ability lies within the FCU with specialist investigators, accountants and analysts, and also houses the Islands Financial Intelligence Unit. The FCU work closely with the Constabulary especially the Drug Trafficking Unit (DTU) in pro-active money laundering investigations involving drugs. It also has access to and liaises closely with other units within the Constabulary such as the Force Intelligence Bureau, Covert Operations and the Constabulary's other investigative wings such as the Criminal Investigation Department. The AG's Chambers provide legal advice and expert assistance in all

financial investigations including money laundering and terrorism financing. There are currently two full time dedicated legal officers.

103. The FCU has a Strategic Board consisting of the Chief Constable, The Collector of Customs and Excise and the AG to whom the Head of the FCU reports.

Police

104. The Constabulary has operational independence and is free from undue political influence or interference. The Isle of Man Constabulary is committed to ensuring that the Isle of Man is not seen as a safe haven for the laundering of money or the financing of terrorism. This is reflected in its Strategic Plan with a key project being 'Strengthening the Financial Crime Unit' and within its Command Teams priorities is the development of a Joint Intelligence Unit.

Financial sector bodies

Financial Supervision Commission (FSC)

105. The FSC is the regulatory authority for all financial institutions other than insurance and pensions businesses. It also authorizes and supervises TSPs and CSPs. The FSC's regulatory objectives are –

(a) securing an appropriate degree of protection for the customers of persons carrying on a regulated activity;
(b) the reduction of financial crime; and
(c) supporting the Island's economy and its development as an international financial center.

106. The FSC is required by law to maintain arrangements to determine whether persons on whom requirements are imposed under the Financial Services Act are complying with them. The FSC is also required to maintain arrangements for enforcing provisions of or under the Financial Services Act or other legislation specified in that Act (Schedule 1 paragraph. 5 of the Financial Services Act 2008). This statutory requirement extends to the Rule Book including the AML/CFT requirements in Part 9 of the Rule Book. The supervision of entities regulated by the FSC is undertaken through a combination of off-site reviews and analysis and on-site inspection visits.

Insurance and Pensions Authority (IPA)

107. The IPA is a statutory board established under the Insurance Act 2008[9] and has responsibility for the regulation of the insurance and pensions sector in the Isle of Man. In carrying out his duties the Supervisor is required to exercise his powers in a way that meets the regulatory objectives set out in the Insurance Act, which are as follows:-

(a) The securing of an appropriate degree of protection for policyholders;

[9] The Insurance Act 2008 is an amalgamation of previously-issued insurance acts and the powers provided to the IPA remain unchanged under the 2008 Act.

(b) The maintenance of confidence in the Island's insurance industry in the Island and elsewhere; and
(c) The reduction in the extent to which it is possible for any insurance business to be used for a purpose connected with financial crime.

108. The supervision of entities regulated by the IPA is undertaken through a combination of both off-site reviews and analysis and on-site inspection visits. As can be seen from the regulatory objectives set out above, the supervisory framework includes responsibility for the matters in relation to AML and CFT.

DNFBP and other matters

Gambling Supervision Commission

109. The Gambling Supervision Commission (GSC) is a body corporate initially established in 1962 and which consists of a Chairman and four members, appointed by the Council of Ministers of the Isle of Man Government. The GSC undertakes the offsite and onsite supervision of the terrestrial casino and on-line casinos.

Financial Supervision Commission – Companies Registry

110. The FSC is responsible for the Isle of Man Companies Registry. This is where Isle of Man incorporated companies are registered and where statutory company documents are filed for public viewing. Companies Registry is also responsible for the administration of legislation relating to foreign companies, limited liability companies, business names, limited partnerships and societies incorporated under the Industrial and Building Societies Acts. In addition to facilitating physical access by the public to the Registry, the authorities have also provided for online access to the records through the internet.

Approach Concerning Risk

111. The IOM has recently adopted a risk-based approach to the application of AML/CFT measures, following the enactment of the FSA, 2008 with effect from August 1, 2008. In order to fulfill the objective of the reduction of financial crime, the FSC has supplemented the AML Code 2008 with Part 9 of the Financial Services Rule Book 2008 ("Rule Book") which concerns money laundering and the financing of terrorism. Part 9 of the Rule Book came into effect on August 1, 2008 for all licenseholders. Part 9 of the Rule Book requires licenseholders to adopt a risk based approach to AML/CFT measures. In particular, it requires licenseholders to conduct a risk assessment of their businesses, including on their customers. It requires licenseholders to conduct customer due diligence (CDD) procedures in accordance with the risk assessment. Requirements to conduct enhanced CDD are also covered where there are higher risks identified by the risk assessment. The FSC has also produced a Handbook of guidance in complying with the Rule Book and the AML Code 2008. This Handbook provides guidance on adopting a risk based approach to AML/CFT measures and the factors that licenseholders should consider. All risk assessments conducted by FSC licenseholders should be recorded and documented and fed into the licenseholders' policies, procedures and controls in respect of AML/CFT.

112. In so far as the insurance industry is concerned, the IPA's statutory remit includes the supervision of insurers in respect of AML/CFT compliance. Until 2008 the sector-specific requirements (in addition to the Code) were contained in the Anti-Money Laundering Standards for Insurance Businesses (the "Standards"). With effect from September 1, 2008 the requirements of the Standards have been replaced by AML/CFT regulations and binding guidance under the provisions of Sections 50 and 51 of the Insurance Act 2008[10], namely:

- Insurance (Anti-Money Laundering) Regulations 2008 (IAMLR 2008)
- Guidance Notes on Anti-Money Laundering and Preventing the Financing of Terrorism – for Insurers (long term business) (IGN 2008)

113. These regulations (applicable to all insurers) and binding guidance notes (applicable to insurers writing long term business) introduce a limited degree of flexibility in so far as risk-based assessment is concerned. Common standards and requirements are set out and these measures are required to be applied as standard. An insurance business is permitted to deviate, in limited circumstances and subject to defined criteria, from these standard requirements where the business' risk assessment identifies the circumstances as lower risk. All risk assessments must be fully documented and recorded and the decision to apply reduced customer due diligence must be approved by a senior member of the business' staff. This will allow the IPA to review such records when conducting its on-site visits. Any decision to apply a deviation against a group of policies must be formally approved, and minuted, at a board meeting of the directors. All business is subject to ongoing due diligence and a customer's risk profile may change in which case due attention must be given to current circumstances and appropriate action taken.

Progress Since the Last IMF Assessment

114. The IOM authorities have addressed most of the recommendations of the last AML/CFT assessment. The previous IMF assessment was conducted against the pre-2003 FATF Recommendations. Following the IMF's assessment in 2002 the FSC produced an action plan which is entitled 'FSC Plan in relation to recommendations made by the IMF in Volume II of the IMF Report on the Isle of Man October 2003–progress update July 04'. The FSC has regularly updated this action plan during the period and a copy of the last update document from January 2008 is entitled 'Anti Money Laundering and Criminal Justice Matters Relevant to FSC'. Because the international standards were revised following the IMF's last inspection, the authorities in the IOM have focused on the revised international standards.

115. The following update was provided to the assessors by the IPA in respect of insurance business:

[10] The Insurance Act 2008 came into force on December 1, 2008, prior to which Sections 24C and 32 of the Insurance Act, 1986 (as amended) provided the IPA with the same powers to issue regulations and binding guidance with regard to AML/CFT.

IMF ASSESSMENT 2002: FATF / ANTI-MONEY LAUNDERING (IPA MATTERS)

Issue	Action	Government Body	Schedule for Implementation
Record Keeping Rules	Expand CTP to include specific requirements for the verification standards. Expand CTP to include a requirement for Insurance Businesses to have a program in place for retrospective review all existing client files.	IPA	Completed
Review of Anti-Money Laundering Code	Review of the Anti-Money Laundering Code 1998. With principal new provisions: • a continuing obligation is to be imposed on relevant businesses to verify evidence of identity as soon as reasonably practical after: The intermediary becomes aware of anything which causes it to doubt the identity of the person who, in relation to the formation of the business relationship, was the applicant for business. • Relevant businesses to ensure that branches and subsidiaries outside the IOM will undertake AML procedures that are no less strict than those that are operated by the relevant businesses. • Where body corporate are applicants for business, a requirement for evidence verifying the existence of a body corporate, its place of incorporation and its corporate nature.	IPA/FSC/ DHA	Completed – all points addressed either in the Anti-Money Laundering Code 2007 or sector-specific Regulations and Guidance Notes.
Review of Anti-Money Laundering Guidance	Inclusion of a provision in the guidance notes to cover the requirement to impose standards of AML/CFT to branches etc outside the IOM.	FSC/IPA	Completed. Updated guidance notes were issued in April 2003. These provisions were further updated in new regulations/guidance in 2008
Power to impose regulatory sanctions and remove auditors	Expand legislative framework to include the power to remove or disqualify an auditor and the power to impose civil money penalties (administrative fines) against individuals, such as directors, officers and controllers, as well as legal persons.	IPA	Completed. Provisions contained in the Insurance (Amendment) Act 2004 and will shortly be consolidated in the Insurance Act 2008
Authority to issue Anti-Money Laundering Guidance Notes	Consider amending relevant laws to clarify legal authority for the IPA to issue guidance notes and regulation on AML matters.	IPA	Completed. Contained in the Insurance (Amendment) Act 2004 and consolidated in the Insurance Act 2008

Issue	Action	Government Body	Schedule for Implementation
Requirement to appoint a AML/CFT compliance officer.	Consider a requirement to designate an AML/CFT compliance officer for FIs other than banks. In addition a requirement for FIs to report a change in such position to the regulator.	FCU/IPA	Completed.
Regulators staffing Resources	IPA and FSC should increase their staffing levels to ensure that they can sustain comprehensive surveillance of all FIs.	FSC, IPA and Treasury	Ongoing review of resources.

2. LEGAL SYSTEM AND RELATED INSTITUTIONAL MEASURES

Laws and Regulations

2.1. Criminalization of Money Laundering (R.1 & 2)

2.1.1. Description and Analysis

Legal Framework:

116. The Isle of Man (IOM) has criminalized money laundering through the Criminal Justice Act 1990 (CJA 1990), the Drug Trafficking Act 1996 (DTA 1996) and the Anti-Terrorism and Crime Act 2003 (ATCA 2003). Whereas the offense defined in the CJA 1990 covers money laundering related to all predicate offenses, the DTA 1996 and ATCA 2003 are limited in scope to predicate offenses involving drug trafficking and terrorism.

117. A legislative package of amendments and consolidation has been adopted by Tynwald in the form of the Proceeds of Crime Act 2008 (POCA 2008). Some provisions of the POCA 2008, as outlined in the relevant sections of this report, came into force on October 22, 2008. The remaining parts of the POCA 2008 are effective from August 1, 2009.[11]

Criminalization of Money Laundering (c. 1.1—Physical and Material Elements of the Offense):

118. As a Crown Dependency, the IOM is not a sovereign State and can therefore not sign or ratify international conventions in its own right. Rather, the United Kingdom (UK) is responsible for the IOM's international affairs and, following consultation with and approval by the IOM Government, it may arrange for the ratification of any convention to be extended to the IOM.

119. Whereas the UK's ratification of the Vienna Convention was extended to the IOM on December 2, 1993, the Palermo Convention has not yet been extended. The mission was informed that the UK would only agree to extend Conventions to the IOM once it was content that the necessary legislative changes to ensure full compliance with their provisions had been made. At the time of the onsite mission there was no concrete timeframe for a request for extension of the Palermo Convention. The IOM was, however, in the process of making the necessary legislative changes to ensure compliance with the provisions of the Palermo Convention and therefore allow for its extension at some point in the future.

120. As indicated above, the IOM's money laundering offenses are defined through three different Acts: the CJA 1990, the DTA 1996, and the ATCA 2003. Whereas the offenses contained in the CJA 1990 and DTA 1996 vary only in terms of scope but not with respect to the material elements, the ATCA's money laundering offense is different also in terms of language and will therefore be discussed separately.

---

[11] Although these parts of the POCA 2008 were not in effect within the timeframe of this assessment, the assessors were in a position to confirm the content of the provisions. Therefore, although not forming part of the assessment, reference is included to them in the relevant sections of the report, mainly by way of footnote.

121. The three strand approach to the IOM's ML offenses remains effective until replaced on August 1, 2009 by Part 3 of POCA 2008. The provisions of the new Act will codify and update the law in relation to ML and no longer differentiate between the predicate offenses of drug trafficking, terrorism, and other crimes.

CJA 1990 and DTA 1996

122. The money laundering offenses of the CJA 1990 extend to all offenses triable on information other than drug trafficking offenses or offenses under the ATCA 2003 as well as to any offenses prescribed by law to be predicate offenses for money laundering. In comparison, the money laundering offenses of the DTA 1996 only relate to certain offenses defined in the Misuse of Drugs Act 1976 and the Customs and Excise Management Act 1986.

123. Sections 17C CJA 1990 and 45 DTA 1996 provide that a person is guilty of money laundering if he (1) conceals or disguises any property which is, or in whole or in part directly or indirectly represents, his proceeds of criminal conduct/drug trafficking or converts or transfers that property or removes it from the jurisdiction for the purpose of avoiding prosecution for an offense or if he (2) knows or has reasonable grounds to suspect that any property is, or in whole or in part directly or indirectly represents, another person's proceeds from criminal conduct/drug trafficking and conceals or disguises that property or converts or transfers that property or removes it from the jurisdiction for the purpose of assisting any person to avoid prosecution for an offense/a drug trafficking offense. Sections 17C (3) and 45 (3), respectively, further state that the reference to concealing or disguising any property include references to concealing or disguising the nature, source, location, disposition, movement or ownership or any rights with respect to it.

124. Articles 17C CJA 1990 and 45 DTA 1996 provide criminal liability for the acts of "concealing or disguising" and the "converting or transferring" only if the prosecution can show that the purpose of the act is to avoid prosecution for a predicate offense. In comparison, the offenses of "conversion or transfer of criminal proceeds" as defined in the Palermo and Vienna Conventions are broader and require proof that the purpose of the act is either to conceal or disguise the illicit origin of the property or to help any person to evade criminal liability for the predicate offense. In addition, under the Vienna and Palermo Conventions, no specific purpose has to be proven for the "concealment or disguise" of the true nature, source, location, disposition, movement, or ownership of or rights with respect to criminal proceeds. Therefore, Articles 17C CJA 1999 and 45 DTA 1996 are not sufficiently wide to meet fully the international standard due to the requirement to prove the outlined purpose in all cases.

125. While certain situations in which a purpose cannot be proven by the IOM prosecutor could be covered by the offense of "assisting another to retain the benefit" of the commission of a predicate offense, the latter offense does not extend to self-laundering as outlined below and also requires proof of the existence of an "arrangement."

126. Sections 17B CJA 1990 and 47 DTA 1996 provide that "a person is guilty of an offense if, knowing that any property is, or in whole or in part directly or indirectly represents another person's proceeds of criminal conduct/drug trafficking, he acquires or uses that property or has possession of it", whereby it is expressly stated that "having possession of any property shall be taken to be doing an act in relation to it." Sections 17B (3) and 47(3), respectively, further provide that it is a defense to

a charge if a person acquired or used the property or had possession of it for adequate consideration, whereby he/she "acquires property for inadequate consideration if the value of the consideration is significantly less than the value of the property" and "uses or has possession of property for inadequate consideration if the value of the property is significantly less than the value of his use or possession of the property." The exception, although a defense for situations in which adequate consideration was provided, is beyond the standard as set forth in the Vienna and Palermo Conventions.

127. IOM law provides that a defendant is guilty of an offense only if the prosecution proves beyond reasonable doubt that each constituent part of the offense has been made out in relation to the defendant. Where the statute provides for a defense, the standard of proof imposed on the defendant is the lesser standard of a balance of probabilities. Thus, if a defendant raises a statutory defense, the prosecution must negate that defense beyond reasonable doubt, otherwise the defendant is entitled to be acquitted. This is a concern with respect to Sections 17B (3) CJA 1990 and 47(3) DTA 1996 as it is not required that the defendant establish that he was bona fide at the time of acquisition or use or having possession of criminal property. The defense of having given adequate consideration would therefore be available even in situations where the defendant knew that the property stems from the commission of a predicate offense.

128. In addition to the above discussed provisions, Sections 17A CJA 1990 and 46 DTA 1996 provide that a person is guilty of money laundering if he enters into or is otherwise concerned in an arrangement whereby the retention or control by or on behalf of another (A) of A's proceeds of criminal conduct/of drug trafficking is facilitated or A's proceeds of criminal conduct/drug trafficking are used to secure that funds are placed at A's disposal or used for A's benefit to acquire property by way of investment and if he knows or suspects that A is or has been engaged in criminal conduct/drug trafficking or has benefited from criminal conduct/drug trafficking. While the first part of the provision overlaps to a large extent with Section 17C CJA 1990 and 45 DTA 1996, the authorities stated that the second part of this provision was intended to be used in money laundering cases involving professionals, such as trustees or lawyers. In practice, the provision has never been tested before the courts.

129. Therefore, even though the outlined provisions cover all the material elements of the money laundering offenses as defined in the Palermo and Vienna Conventions, the assessors are concerned that the defense in Sections 17B (3) CJA 1990 and 47 (3) DTA 1996 may be open to abuse by money launderers to avoid criminal liability for the acquisition, possession, or use of criminal proceeds.

ATCA 2003

130. Terrorism financing offenses are explicitly excluded from the scope of the CJA 1990 and money laundering offenses based on terrorism financing may therefore not be prosecuted under the above-cited provisions. The ATCA 2003 itself, however, contains a money laundering provision applicable to terrorism related predicate offenses.

131. Pursuant to Section 10 ATCA 2003 it is an offense to enter into or become concerned in an arrangement which facilitates the retention or control by or on behalf of another person of terrorist property, including through concealment, removal from the jurisdiction, the transfer to nominees or through any other way. In discussions with the authorities it was clarified that the elements of the

offense that have to be proven by the prosecution are (1) the existence of a written, oral, or implied arrangement (2) that the arrangement facilitates the retention or control of another's terrorist property and (3) that the perpetrator knew or should have known at the time the arrangement was made that the property constituted terrorist property.

132. While Section 10 ATCA 2003 covers some of the material elements of the money laundering offenses as defined in the Vienna and Palermo Conventions, the requirement to prove all three elements as indicated above will prevent the application of the provision to all situations required by the Conventions. For example, the offense would not cover situations in which a person converts or transfers criminal proceeds for the purpose of disguising or concealing the illicit origin of the property unless the existence of an arrangement can established beyond a reasonable doubt. Equally, situations in which a person conceals or disguises the true nature, source, location, disposition of, or rights with respect to proceeds of crime would not be covered unless all three elements of the offense can be established.

The Laundered Property (c. 1.2):

133. Sections 17A CJA 1990 and 46(2) DTA 1996 define "proceeds" as "any property which in whole or in part, directly or indirectly, represent…proceeds of criminal conduct". Sections 22 CJA 1990 and 57 DTA 1996 further specify that "property" includes money and all other property, real or personal, heritable or moveable, including things in action and other intangible or incorporeal property, whereby property is considered to be held by a person who has an interest in it, including rights. Sections 22 CJA 190 and 57 DTA 1996 further state that "property" includes all property, whether it is situated in the Island or elsewhere.

134. Equally, Section 6 ATCA 2003 defines "terrorist property" as any property, which wholly or partly, directly or indirectly represents the proceeds of acts of terrorism, including payments or other rewards in connection with its commission. Section 75 ATCA 2003 further stipulates that "property" includes property wherever situated and whether real or personal, heritable or moveable, and things in action and other intangible or incorporeal property.

135. Both the money laundering offenses of the CJA 1990/DTA 1996 and the ATCA 2003 therefore, extend to any type of property, regardless of its value, that are derived from or obtained, directly or indirectly, through the commission of a criminal offense, including assets of every kind, whether corporeal or incorporeal, moveable or immoveable, tangible or intangible, and legal documents or instruments evidencing title to, or interest in such assets.

Proving Property is the Proceeds of Crime (c. 1.2.1):

136. The language of the provisions in the CJA 1990, the DTA 1996 and the ATCA 2003 do not require a conviction for a predicate offense to prove that certain property constitutes proceeds of crime. While the law is silent on the standard of proof applicable to establish that property stems from an illegal source, the authorities stated that it would have to be established "beyond a reasonable doubt" that property stems from a specific predicate offense.

137. Theoretically, cases could arise in which evidence relating to the commission of a predicate offense may suffice to satisfy the required burden of proof even in the absence of a conviction for a

predicate offense. In practice, however, it would appear very difficult to do so, in particular with respect to cases involving offenses committed extraterritorially where evidence gathering is conducted almost exclusively through international cooperation.

138. The authorities confirmed that the difficulties in obtaining sufficient evidence to meet the high standard of proof applicable to establish that the property in question is of criminal origin is one of the main challenges in obtaining convictions for the stand alone money laundering offense, particularly in cases where the predicate offense has been committed abroad.

The Scope of the Predicate Offenses (c. 1.3):

139. As indicated above, the money laundering offenses of the CJA 1990 extend to offenses prescribed to be predicate offenses for money laundering and all offenses triable on information other than a drug trafficking offense or an offense under the ATCA 2003. So far, no offenses have been prescribed to constitute predicate offenses for money laundering.

Predicate Offense	Law
Participation in an organized criminal group and racketeering	While there are no separate predicate offenses, the category is covered through the offense of “conspiracy” as defined in Section 330 Criminal Code 1872.
Terrorism, including terrorism financing	Sections 7, 8, 9, 10, 11, and 14 ATCA 2003.
Trafficking in human beings and migrant smuggling	Sections 25 Immigration Act 1971 applicable through Immigration (Isle of Man) Order 1991.
Sexual exploitation, including sexual exploitation of children	Sections 1-31 Sexual Offenses Act 1992.
Illicit trafficking in narcotic drugs and psychotropic substances	Sections 4, 5, 6, 8, 9, 11, 12, 13, 17, 18, 20, 23 Misuse of Drugs Act 1976.
Illicit arms trafficking	Section 47, 69 and 179 Customs and Excise Management Act 1986, Import of Goods (Control) Order 1954, Export of Goods (Control)(Application) Order 2004, and Trade in Controlled Goods (Control) Order 2004.
Illicit trafficking in stolen and other goods	Section 24 Theft Act 1981.
Corruption and bribery	Section 323 Criminal Code 1872, Sections 1, 2, 3, 6, 7 Corruption Act 2008.
Fraud	Sections 14, 15, 15A, 16, 17 and 23 Theft Act 1981.
Counterfeiting Currency	Sections 1, 2, and 3 Coinage Offenses Act 1980.
Counterfeiting and piracy of products	Section 106 Copyright Act 1991, Section 176 Customs and Excise Management Act 1986.
Environmental crime	Section 3 Water Pollution Act 1993.
Murder, grievous bodily injury	Sections 18-20 Criminal Code 1872
Kidnapping, illegal restraining and hostage-taking	Sections 60B, 60C, 60D Criminal Code 1872.
Robbery or theft	Sections 7, 8, 9, 10, 11, 12 Theft Act 1982.
Smuggling	Sections 47(2) and (3), 69 (2), and 178 Customs and Excise Management Act 1986.
Extortion	Section 23 Theft Act 1981.
Forgery	Sections 2, 3, 4 and 5 Forgery Act 1952.
Piracy	Sections 2 and 4 Piracy Act 1837.
Insider trading and market manipulation	Section 1 Insider Dealing Act 1998.

140. There is no statutory offense of tax evasion in the IOM, although failure to submit a tax return or delivery of an untrue return is an offense under Section 108 of the Income Tax Act. While tax evasion could constitute the offence of "false accounting" pursuant to Article 19 Theft Act 1981 (which is a predicate offense for money laundering), no such prosecutions have been taken.

141. All FATF-designated categories of predicate offenses are covered, as outlined above, under IOM law.

Threshold Approach for Predicate Offenses (c. 1.4):

142. The IOM´s legal system differentiates between two categories of crimes: Offenses triable on information and offenses tried summarily. Unlike the UK, the IOM does not rely on common law offenses but defines all criminal offenses through statute.

143. There is no general provision in any Act that would categorize crimes into "offenses triable on information" and "summary offenses". Rather, each statutory offense indicates whether or not it may be tried summarily or on information or both. Generally, offenses punishable with more than six months constitute "offenses triable on information" while all others are considered "summary offenses." In very limited circumstances and only with respect to offenses listed in the Summary Jurisdiction Act 1989 (Schedule 2) may an offense triable on information be dealt with summarily.

144. The IOM has adopted a threshold approach for predicate offenses based on category. Section 1(9)(c) CJA 1990 which provides that certain offenses designated by law ("prescribed offenses") as well as all offenses triable on information other than drug trafficking and terrorism offenses, which are dealt with specifically in the DTA 1996 and the ATCA 2003, constitute predicate offenses for money laundering. The provision further clarifies that the reference to "all offenses triable on information" would extend to offenses that may be tried summarily pursuant to Schedule 2 Summary Jurisdiction Act 1989.

145. All money laundering offenses of the CJA 1990, the DTA 1996 and the ATCA 2003 provide for sanctions both for summary convictions and convictions on information. Their categorization therefore depends on the circumstances of each specific case. The authorities stated, however, that in practice all charges for money laundering would be brought before the High Court as the punishment applied for is generally too high for adjudication by the summary court.

Extraterritorially Committed Predicate Offenses (c. 1.5):

146. All three statutes defining money laundering offenses cover both conduct which constitutes a predicate offense on the IOM or any conduct committed abroad that would have constituted a predicate offense had it occurred in the IOM (Sections 17A (7) CJA 1990, 1(1)(f) DTA 1996, 1(4)(a) ATCA 2003). Dual criminality is not required. There are also no jurisdictional provisions that would require any other link between the IOM and the perpetrator, such as citizenship or residence as long as the laundering offense has been committed in the IOM.

Laundering One's Own Illicit Funds (c. 1.6):

147. Sections 17C CJA 1990 and 45 DTA 1990 make it an offense for a person to conceal, disguise, transfer, or convert criminal proceeds both in cases where the property stems from the commission of a predicate offense by another or by the person himself.

148. The acquisition, possession or use of proceeds of criminal conduct, however, is only criminalized if the property involved stems from another person's criminal behavior and does not extend to self laundering. While Section 2 Criminal Law Act 1981 provides for the principle of "ne bis in idem" it does not appear that the principle would prevent the criminalization of self-laundering involving the listed acts constituting money laundering. This view is also supported by the fact that Tynwald, in the course of the first reading of the draft, did not comment on or request a change of the provisions in the Proceeds of Crimes Bill 2008 providing for a self laundering offense relating to the acquisition, possession and use of criminal proceeds. The authorities stated that while the principle of double jeopardy would not per se prevent the criminalization of self laundering for "acquisition, possession and, use", with the coming into force of the POCA 2008 from August 1, 2009 and to avoid a violation of Section 3 Criminal Law Act 1981 the prosecution will have to make a choice as to which provision will be used to bring charges: either the predicate offense or the self laundering offense.

149. The ATCA 2003 does not extend the money laundering offense to situations where the terrorist or terrorist financer himself conceals or transfers property to maintain control over it. Rather, the offense only covers persons who do so for or on behalf of somebody else.

Ancillary Offenses (c. 1.7):

150. Ancillary offenses are criminalized under the general provisions of the Criminal Code 1872.

151. Section 9 Criminal Law Act 1981 provides that unless otherwise stated, sanctions for commission of an offense shall not only be applied to completed but also to attempted crimes, whereby a crime is considered attempted if the perpetrator carries out an overt act that goes beyond mere preparation.

152. Conspiracy is covered through Section 330 Criminal Code 1872. Pursuant to the provision, if two or more persons conspire to commit any offense, such persons shall be held criminally liable and may be punished with imprisonment for a term not exceeding ten years.

153. Furthermore, Sections 350 and 351 Criminal Code 1872 provide for criminal liability of any person who is accessory before the fact to any felony or who counsels, procures, or commands another to commit any felony. Both sections provide that the accused may be punished as if he were the principal offender.

154. IOM law therefore allows for the prosecution of all parties that may be involved in the commission of the money laundering offense.

Additional Element—If an act overseas which do not constitute an offense overseas, but would be a predicate offense if occurred domestically, lead to an offense of ML (c. 1.8):

155. As indicated above, all three statutes define money laundering to cover both conduct which constitutes a predicate offense in IOM or would have constituted a predicate offense had it occurred in the IOM (Sections 17A(7) CJA 1990, 1(1)(f) DTA 1996, 1(4)(a) ATCA 2003). Dual criminality is not required.

Liability of Natural Persons (c. 2.1):

156. The three money laundering offenses as outlined above are offenses for which intent is required and therefore apply to persons who knowingly engage in the conduct in question. With respect to the property in question the required mental element varies depending on the actus reus.

157. With respect to the acts of concealing, disguising, converting or transferring of criminal proceeds, a person may be held criminally liable if the prosecution can establish beyond a reasonable doubt that the person knew or objectively should have known that the property in question stems from the commission of a crime.

158. For the offense relating to the acquisition, possession, or use of criminal proceeds, the required mens rea is actual knowledge that the property in questions constitutes criminal proceeds.

159. For the acts of assisting another person to retain the benefit of crime it suffices that the prosecution can establish beyond a reasonable doubt that the perpetrator knew or suspected that the person he/she entered into an agreement with is or has been engaged in criminal conduct. While it is not required that the prosecutor establishes the perpetrator's actual knowledge about the criminal source of the property involved, the defendant has a defense and therefore a right to acquittal if he/she can establish by balance of probability that he did not actually have knowledge of the criminal nature of the property in question.

160. For money laundering based on the predicate offense of terrorism or terrorism financing, the ATCA 2003 does not expressly stipulate a mental element requirement with respect to the nature of the property but provides that the defendant has a defense if he/she can prove by a balance of probability that he did not know and objectively had no reasonable cause to suspect that the arrangement related to terrorist property.

161. At a minimum and with respect to all acts constituting money laundering a person may therefore be held criminally liable for money laundering if he acted intentionally and with the knowledge that the property involved stems from a criminal source. The Vienna and Palermo Conventions set forth a minimum standard that the perpetrator acts in the knowledge that the laundered property is the proceeds of crime. Intent as defined in IOM law therefore meets the international standard with respect to the mental element requirement.

The Mental Element of the ML Offense (c. 2.2):

162. None of the three Acts contain a provision clarifying whether or not the mental element may be inferred from objective factual circumstances and at the time of the onsite mission no case law existed in the IOM to clarify that point. However, with respect to all money laundering offenses as outlined above, the English common law principle regarding the ability to make reasonable inferences from objective factual circumstances applies.

163. Additionally, with respect to the acts of concealing, disguising, converting, or transferring of criminal proceeds, it is sufficient for the prosecution to show that the perpetrator objectively should have known that the property in question constitutes proceeds of crime. Therefore, the provision expressly allows for the intentional element of the offense to be inferred from objective factual circumstances.

Liability of Legal Persons (c. 2.3); Liability of Legal Persons should not preclude possible parallel criminal, civil or administrative proceedings & c. 2.4):

164. The money laundering provisions of the CJA 1990, the DTA 1996, and the ATCA 2003 apply to any "person" without differentiating between legal and natural persons. The Interpretation Act 1976, which applies to every provision of every Act passed after May 1949 defines "person" to cover any person, natural or legal.

165. The language of the money laundering offenses does not preclude the possibility of parallel criminal, civil, or administrative sanctions for perpetrators that are legal entities. The authorities confirmed that both criminal and civil/administrative proceedings could be instituted against legal persons at the same time, whereby it was pointed out that in practice it would be more likely that the authorities would institute civil proceedings against the legal person and criminal proceedings against directors or managers of the legal entity in question. At the time of the assessment no legal entity has been held criminally liable for money laundering in the IOM.

Sanctions for ML (c. 2.5):

166. Pursuant to Sections 17A (6), 17B (9), 17C (4) CJA 1990, Section 51(1) DTA 1996, and Section 10 ATCA 2003, the sanctions applicable to both natural and legal persons convicted for money laundering are imprisonment for a term not exceeding six months or a fine not exceeding GBP 5,000 (on summary conviction) or imprisonment for a term not exceeding 14 years or a fine or both (on conviction on information).

167. The sanction for money laundering seems to be in line with other serious crimes under IOM law. For example, fraud and theft may be sanctioned with imprisonment of up to ten years, forgery with imprisonment of up to 14 years and counterfeiting with imprisonment for life.

168. The IOM's sanctions for money laundering are identical with those of the UK.

169. Overall, the statutory sanctions for the money laundering offenses seem to be effective, proportionate and dissuasive.

Analysis of Effectiveness:

170. While representatives of the AG's office provided the assessors with information on the number and nature of money laundering prosecutions and trials, no complete and accurate official statistics on the overall number and nature of investigations and prosecutions, including cases that were subsequently dropped, are being maintained by the IOM authorities.

171. Representatives of the FCU estimated that since 2006 only about six STRs resulted in an investigation.

172. While the overall number of money laundering investigations could not be established, the authorities stated that, since 2003, four cases for general money laundering based on the CJA 1990 have been investigated, all of which related to predicate offenses committed abroad and were subsequently dropped due to the difficulties in obtaining the necessary evidence to show that the proceeds in question constituted criminal proceeds. Two of the investigations were discontinued in 2007 and two in 2008. Of the four investigations, two related to fraud, one to obtaining money by deception, and one to theft.

173. The authorities informed the assessors that at the time of the assessment, four prosecutions for money laundering based on the CJA 1990 were ongoing.

174. Representatives of the AG's Office stated that at the time of the assessment, 16 charges for money laundering have been brought before IOM courts, all of which were filed based on the DTA 1996 and related to drug trafficking predicate offenses. Two cases were filed in 2005, six in 2006, six in 2007, and two in 2008. Of the 16 cases, six resulted in convictions and five are still pending. The remaining five cases resulted in acquittals. All of the convictions were additional to convictions for the predicate offense and the longest sanction imposed for the money launderings charge was two years. No convictions have ever been obtained for autonomous money laundering.

175. At the time of the assessment, charges had been brought in one case under the stand-alone money laundering provision of the CJA 1990. The case, which originated from an STR, had not yet reached trial stage.

176. The low number of STRs resulting in an investigation and ultimately in a prosecution, the low number of convictions, the lack of convictions for the stand-alone money laundering offense, and the relatively mild sanctions imposed by the courts, call into question the effective implementation of the money laundering offense. The authorities explained that in typical money laundering cases the subjects of the STRs do not reside in the IOM and the alleged predicate offense has also been committed outside the IOM. In such circumstances, the IOM authorities must depend on the other jurisdiction(s) involved to obtain the evidence necessary to commence an investigation, which is often a lengthy process, sometimes taking years. For their part, the IOM authorities have been active in sharing relevant information with foreign counterparts to facilitate investigations and prosecutions conducted abroad.

177. The assessors understand that the nature of much of the financial services business conducted in the IOM, involving funds received from abroad on behalf of nonresidents, can make it difficult to prosecute money laundering cases locally and more efficient to transfer cases to other jurisdictions in which the predicate offense may have occurred or the funds or accused persons are located. However, the assessors consider it important that the IOM seeks also to develop its own case law in this area, both to establish that money laundering is a stand-alone offense that may be prosecuted independently from the predicate offense and to clarify the level of proof required to determine that proceeds are illicit and how specific the evidence needs to be in relation to specific predicate offenses. Improving the current level of results from the domestic system represents a challenge that should be addressed by the IOM authorities as a whole.

2.1.2. Recommendations and Comments

- Amend Articles 17C CJA 1990 and 45 DTA 1996 to:
  - provide for two alternative purposes for the acts of converting and transferring proceeds, namely to avoid prosecution for the predicate offense or to conceal the illicit origin of the funds, and;
  - eliminate the purpose requirement for the acts of converting and transferring proceeds of crime.
- The defense (payment of adequate consideration) provided for in Sections 17B(3) CJA 1990 and 47(3) DTA 1996 is not provided for in the Vienna and Palermo Conventions and should be eliminated as it may allow money launderers to abuse the provision to avoid criminal liability for the acquisition, possession, or use of criminal proceeds/proceeds.
- Amend Section 10 ATCA 2003 to cover all material elements of the money laundering provisions of the Palermo and Vienna Conventions.
- Amend the offenses of acquisition, possession, or use in the CJA 1990 and the DTA 1996 as well as the money laundering offense contained in the ATCA 2003 to include criminal proceeds obtained through the commission of a predicate offense by the self launderer.
- The authorities should:
  (i) address any barriers to stand-alone ML prosecutions, including the level of proof needed to determine that property stems from the commission of a specific predicate offense; and
  (ii) take steps to develop jurisprudence on autonomous money laundering to establish that ML is a standalone offense.

2.1.3. Compliance with Recommendations 1 & 2

	Rating	Summary of factors underlying rating
R.1	**PC**	• Articles 17C CJA 1990 and 45 DTA 1996 are not sufficiently wide to fully meet the international standard due to the requirement that acts of "concealing or disguising" and "converting or transferring" are carried out with the purpose of avoiding prosecution for a predicate offense. • The defenses (payment of adequate consideration) provided for in Sections 17B (3) CJA 1990 and 47 (3) DTA 1996 are not provided for in the Vienna and Palermo Conventions and may allow money launderers to abuse the provision to avoid criminal liability for the acquisition, possession, or use of criminal proceeds. • Section 10 ATCA 2003 does not cover all material elements of the money laundering provisions of the Palermo and Vienna Conventions.

		• The offenses of acquisition, possession, or use in the CJA 1990 and the DTA 1996 as well as the money laundering offense contained in the ATCA 2003 do not extend to self-laundering. • The low level of relevant domestic investigations and prosecutions calls into question the effectiveness of the ML offense.
R.2	**LC**	• While statutory sanctions for money laundering are comprehensive, dissuasive and proportional, the number of convictions obtained and the sentences actually imposed by the courts appear rather low. • It is difficult to assess the effectiveness of the stand-alone money laundering offense given that the provision has not yet been tested before the courts. The low number of investigations and prosecutions further supports the conclusion that money laundering is not yet dealt with as a stand-alone offense.

2.2. Criminalization of Terrorist Financing (SR.II)

2.2.1. Description and Analysis

Legal Framework:

178. IOM law criminalizes the financing of terrorism through ATCA 2003 Sections 6–9.

179. As indicated under Recommendation 1, the IOM is a Crown Dependency and cannot sign or ratify international conventions in its own right. Rather, the UK is responsible for the IOM's international affairs and may arrange for any convention's ratification to be extended to the IOM. The UK's ratification of the International Convention for the Suppression of the Financing of Terrorism (FT Convention) has been extended to the IOM on September 25, 2008.

180. Of the other 15 international counter-terrorism related legal instruments, ten have been extended to the IOM, namely the Diplomatic Agents Convention, the Civil Aviation Convention, the Maritime Convention, the Fixed Platforms Protocol, the Convention on the Making of Plastic Explosives for the Purpose of Detection, the Hostage Taking Convention, the Unlawful Seizure Convention, the Aircraft Convention, the Airport Protocol, and the Nuclear Material Convention.

Criminalization of Financing of Terrorism (c. II.1):

181. ATCA 2003 Section 7 is the main terrorism financing offense. The provision makes it an offense for a person to receive or provide or invite another to provide money or other property where the person either intends that the property will be used or has reasonable grounds to suspect that the property may be used for the purpose of terrorism.

182. ATCA 2003 Section 8 criminalizes the use of money or other property for terrorism purposes as well as the possession of money or other property where the person possessing the property either intends to use it for terrorism or has reasonable cause to suspect that it may be used for terrorism.

183. ATCA 2003 Section 9 furthermore provides that it is an offense for a person to enter into or become concerned in an arrangement as a result of which money or property is made available or is to be made available to another and the person knows or has reasonable cause to suspect that it will or may be used for purposes of terrorism.

184. Pursuant to ATCA 2003 Section 6, the term "terrorist property" extends to money or other property that is likely to be used for the purpose of terrorism, including any money or property that is or will be made available for use by proscribed organizations, as well as the proceeds of the commission of terrorist acts and acts carried out for the purpose of terrorism. Section 75 further specifies that "property" includes property wherever situated and whether real or personal, heritable or moveable, and things in action and other intangible or incorporeal property.

185. The international standard requires that the terrorist financing offense extend to any person who provides or collects funds by any means, directly or indirectly, with the intention that they be used for terrorist acts, by a terrorist organization or by an individual terrorist.

Terrorist Acts:

186. ATCA 2003 Section 1 defines "terrorism" as the use or threat of action where (1) the act involves serious violence against a person or property, endangers a person's life other than that of the person committing the act, creates a serious risk to the health or safety of the public or a section thereof, or is designed to interfere with or seriously disrupt an electronic system, and (2) the use or threat is designed to influence a government or to intimidate the public or a section thereof, and (3) for the purpose of advancing a political, religious or ideological cause. If, however, any of the acts listed under (1) involve firearms or explosives and are committed for the purpose of advancing a political, religious, or ideological cause, it is considered terrorism regardless of whether the requirements listed in (2) are met.

187. Under the FATF standard, "terrorist acts" include (1) offenses as defined in the nine Conventions and Protocols listed in the Annex to the FT Convention and (2) any other act intended to cause death or serious bodily injury to a civilian, or to any other person not taking an active part in the hostilities in a situation of armed conflict, when the purpose of such act, by its nature or context, is to intimidate a population, or to compel a Government or an international organization to do or to abstain from doing any act."

188. With respect to the generic terrorism offense it would appear that the scope of ATCA 2003 Section 1 covers all but one aspect of the FATF definition. While the latter is limited to acts against civilians, the former covers violence against any person or property as long as the act is designed to influence a government or intimidate the public. However, while the FATF definition also includes acts designed to intimidate an international organization, no such reference to international organizations is contained in the ATCA 2003.

189. As indicated above, for the generic offense, IOM law provides that only acts undertaken or threats made with the intention of advancing a political, religious, or ideological cause would constitute "terrorism." This approach, which adds an element not set forth directly in the FT Convention, is one that a number of countries have adopted to ensure the generic definition is not used in circumstances where it was not intended. The authorities should assess the advantage of this approach in the domestic context 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.

190. ATCA 2003 Section 1 does not contain an express reference to the offenses defined in the nine Conventions and Protocols listed in the Annex to the FT Convention. To satisfy the requirements of the international standard on that point, the generic terrorism offense would therefore have to be broad enough to cover all offenses defined in the nine Conventions and Protocols. However, while the use or threat with the use of serious violence is required for an act to fall under the definition of ATCA 2003 Section 1 as outlined above, some of the offenses in the Conventions and Protocols do not require the use of violence or threat thereof. For example, the Nuclear Material Convention makes it a terrorism offense to possess nuclear material if the prescribed mental element is met.

191. In practice the scope of the terrorism offense in the ATCA 2003 may therefore cover many but clearly does not extend to all "terrorist acts" as defined in the FATF standard.

Terrorist Organizations:

192. ATCA 2003 Section 1(5) provides that any reference to "action taken for the purpose of terrorism" would include action taken for the benefit of a proscribed terrorist organization. ATCA 2003 Sections 7–9 therefore apply to the provision or collection of funds for the benefit of proscribed terrorist organizations, whereby an organization is proscribed if it is listed in Schedule 2 to the Terrorism Act 2000. The ATCA does not provide for a definition of "terrorist organization".

193. To some extent ATCA 2003 Section 7 also applies to situations where a person collects or provides funds that he/she has reasonable cause to suspect may be used for terrorism. If a person funds a terrorist organization not "proscribed" by Parliament, it is assumed that he/she has reasonable cause to suspect that the money may be used for terrorism and may therefore be held criminally liable for terrorism financing.

194. However, the terrorism financing provisions of the ATCA 2003 have never been tested before the courts and it has not been established in what circumstances property is considered to be "used for terrorism". It is therefore unclear whether the financing of terrorist organizations could be prosecuted under the cited provisions in cases where the support relates to costs of living, education expenses or similar expenses.

Individual Terrorists:

195. The ATCA 2003 does not expressly criminalize the financing of individual terrorists, nor does it contain a definition of the term "terrorist". However, Sections 7-9 ATCA 2003 extend to situations where a person collects or provides funds that he/she has reasonable cause to suspect may be used for terrorism. The authorities have indicated that in the IOM, if a person provides funds to an

individual terrorist, he/she would be assumed to have reasonable cause to suspect that the money "may" be used for terrorism and could therefore be held criminally liable for terrorism financing.

196. The standard of "reasonable cause to suspect" that the funds "may" be used for terrorism is a relatively low one. Nonetheless, it is not clear that the provision of living and private expenses to an individual terrorist would be covered by the IOM's provisions, as interpreted by a court. The assumption is not set forth in the statutory language. Even if the court were to assume this, evidence can be adduced to rebut that assumption. There is no jurisprudence on the issue. In addition, for the reason outlined above, such situations would not necessarily be covered by the ancillary offenses. However, provision of any funding to such individuals is a criminal offense under the Al-Qa'ida and Taliban (UN Measures) (Isle of Man) Order 2002 and the Terrorism (UN Measures)(Isle of Man) Order 2001 respectively and prosecutions in the IOM could be initiated directly based on the provisions of those Orders. The latter not only applies to individuals and entities designated pursuant to UN Resolution 1373 but extends to any person within the IOM and any British citizen elsewhere who is ordinarily residing in the IOM or body corporate established under IOM law. With these provisions and the possibility that the funding would also be captured by Sections 7-9 ATCA 2003, IOM has clear avenues to impose criminal liability for the funding of the living and private expenses of individual terrorists.

197. ATCA 2003 Section 7(4) provides that a reference to the "provision of money" would include money or other property given, lent or otherwise being made available, whether or not for consideration. Section 75 further provides that "property" extends to property wherever situated, whether real or personal, heritable or moveable, and things in action and other intangible or incorporeal property. The language of the provision is not limited to property that stems from illegitimate sources and the authorities confirmed that terrorism property as defined in Section 6 in connection with Section 75 ATCA would extend property from illegal as well as legitimate sources.

198. The terrorism financing provisions do not require that the funds provided are actually used to carry out or attempt the commission of a terrorist act or that the funds are linked to a specific terrorist act. It is merely required that the funds are intended for use in the commission of a terrorist act or that the financer has reasonable cause to believe that they will be used for terrorism or for the benefit of a proscribed terrorist organization.

199. ATCA 2003 does not define any ancillary offenses for terrorist financing. However, the general provisions of the Criminal Code 1872 also apply with respect to the terrorism financing offense.

200. Criminal Law Act 1981 Section 9 provides that unless otherwise stated, sanctions for the commission of an offense shall not only be applied to completed but also to attempted crimes, whereby a crime is considered attempted if the perpetrator carries out an overt act that goes beyond mere preparation.

201. Conspiracy is covered through Criminal Code 1872 Section 330. Pursuant to the provision, if two or more persons conspire to commit any offense, such persons shall be held criminally liable and may be punished with imprisonment for a term not exceeding ten years.

202. Furthermore, Criminal Code 1872 Sections 350 and 351 provide for criminal liability of any person who is accessory before the fact to any felony or who counsels, procures, or commands another to commit any felony. Both sections provide that the accused may be punished as if he were the principal offender. IOM law therefore allows for the prosecution of all parties that may be involved in the commission of a terrorism financing offense.

Predicate Offense for Money Laundering (c. II.2):

203. As outlined under section 1.1 of this report, offenses under the ACTA 2003 are expressly excluded from the money laundering offenses of the CJA 1990. However, the ATCA 2003 itself, through Section 10, contains a money laundering offense which is exclusively applicable to situations in which the funds involved constitute terrorist property. Further information on the elements as well as the shortcomings of the ATCA money laundering offense may be found in Section 1.1.

Jurisdiction for Terrorist Financing Offense (c. II.3):

204. ATCA 2003 Section 49 provides that a person may be held criminally liable for any acts committed outside the IOM that would have constituted a terrorist offense pursuant to ATCA 2003 Sections 7–10 had they been committed in the IOM. Furthermore, the term "action" includes any action outside the island, "the public" extends to the public of the IOM as well as of a country or territory other than the IOM and "the government" refers to the government of the IOM, of the UK, or of any other country or territory.

205. The terrorist financing offenses of the ATCA 2003 therefore apply regardless of whether the person alleged to have committed the offense is in the same or a different country from the one in which the terrorist or terrorist organization is located or the terrorist act occurred or will occur. There are also no jurisdictional provisions that would require any other link between the IOM and the perpetrator, such as citizenship or residence.

The Mental Element of the TF Offense (applying c. 2.2 in R.2):

206. As outlined above, the terrorism financing offense under the ATCA 2003 requires that the perpetrator either knows or intends that the funds are being used for a terrorist act or has reasonable cause to believe that they may be used for terrorism purposes, including for the benefit of proscribed terrorist organizations.

207. As in the case of CJA 1990 and DTA 1996, ATCA 2003 does not expressly provide that the intentional element required for the commission of the terrorism offense may be inferred from objective factual circumstances. However, the English common law principle regarding the ability to make reasonable inferences from objective factual circumstances applies also with respect to the terrorism financing offense.

Liability of Legal Persons (applying c. 2.3 & c. 2.4 in R.2):

208. The terrorism financing offenses of ATCA 2003 apply to any "person" without differentiating between legal and natural persons, whereby Section 1(4)(b) provides that the reference extends to any person, wherever situated. The Interpretation Act 1976, which applies to "every provision of every Act passed after May 1949" defines "person" to cover any person, natural or legal.

209. The language of the ATCA 2003 would suggest that criminal liability of legal persons for any FT offense would not preclude the possibility of parallel criminal, civil, or administrative sanctions for terrorist financers that are legal entities and the authorities confirmed that both criminal and civil/administrative proceedings could be instituted against legal persons at the same time. It was pointed out that, in practice, it would be more likely that the authorities would institute civil proceedings against the legal person and criminal proceedings against directors or managers of the legal entity in question. At the time of the assessment no legal entity has been held criminally liable for FT.

Sanctions for FT (applying c. 2.5 in R.2):

210. The sanctions applicable for FT pursuant to ATCA 2003 are imprisonment for a term of up to 14 years or a fine or both (upon conviction) or imprisonment for a term of up to six months or a fine of up to GBP5,000 or both (upon summary conviction). The IOM's sanctions for terrorist financing are identical to those of UK. As there has never been a conviction for FT in the IOM, no sanctions have ever been imposed.

Analysis of Effectiveness:

211. There have been no investigations or prosecutions relating to FT and the FT offense has therefore never been tested before the courts.

2.2.2. Recommendations and Comments

- Amend Article 1 ATCA 2003 to include a reference not only to governments but also to international organizations.
- Amend the definition of "terrorism" in Section 1 ATCA 2003 to extend to all terrorism offenses as defined in the nine Conventions and Protocols listed in the Annex to the FT Convention.
- Consider the impact of including in the FT offense "intention of advancing a political, religious, or ideological cause" on the IOM's ability to successfully prosecute in factual settings contemplated by the FT Convention.

2.2.3. Compliance with Special Recommendation II

	Rating	Summary of factors underlying rating
SR.II	**LC**	• Article 1 ATCA 2003 does not contain a reference to international organizations. • The definition of "terrorism" in Section 1 ATCA 2003 does not extend to all terrorism offenses as defined in the nine Conventions and Protocols listed in the Annex to the FT Convention.

2.3. Confiscation, freezing and seizing of proceeds of crime (R.3)

2.3.1. Description and Analysis

Legal Framework:

212. There is no overarching statutory instrument covering all instances of seizure and confiscation of criminal assets or proceeds in general. Relevant provisions are found in three different Acts: the legislation covering seizure and confiscation of proceeds of crime in respect of ML and FT is currently found in DTA 1996 (confiscation and seizing of the proceeds of drug trafficking offenses), CJA 1990 (confiscation and seizing of the proceeds of all other offenses) and ATCA (freezing and forfeiture of terrorism related assets).

213. Part 1 of the POCA 2008, which came into effect on October 22, 2008, introduced a procedure of civil recovery of illegal proceeds. Part 2 of the POCA 2008 will, once in force in August 2009, streamline and update the legislation in this area. It provides for criminal confiscation and restraint measures in the IOM, replacing the separate drug trafficking and criminal justice legislation with a consolidated set of provisions, but leaves the separate rules for terrorist assets untouched.

Confiscation of Property related to ML, FT or other predicate offenses including property of corresponding value (c. 3.1):

Laundered Property

214. There is no general provision explicitly covering the confiscation of the laundered assets as the object of the (autonomous) money laundering offense ("corpus delicti") in a stand-alone prosecution. It is argued that the "object" of a money laundering offense is seen as the "proceeds" of crime and any application for restraint or confiscation of such "proceeds" of crime would be made under the relevant sections of the Criminal Justice Act/Drug Trafficking Act or Proceeds of Crime Act accordingly. So arguably the CJA 1990 and the DTA 1996 implicitly provide for the value-based confiscation of the object of the offense as this measure is applied to any benefit gained from criminal conduct, once the court has established that such conduct has occurred and has generated proceeds that have subsequently gone through a laundering process. This opinion is however a matter of debate and has not yet been tested in a stand-alone ML prosecution, nor confirmed in authoritative doctrine.

Proceeds

General Regime

215. Except for drug trafficking and terrorism related cases, the relevant provisions of CJA 1990 Part 1 apply. A confiscation order is issued by either the Summary or the High Court upon conviction, ordering the defendant to pay a sum "as the court thinks fit". The offender has to be found guilty of an offense, namely a prescribed offense (i.e., prescribed by order of the DHA)12 or of another offense, except if it is a drug trafficking offense under DTA 1996 or an offense under ATCA

[12] No such orders have been issued yet.

2003. The Court has to be satisfied that the offender has benefited from that offense or from that offense together with any other offense for which he is convicted in the same proceedings.

216. 'Benefiting from crime' is defined as obtaining property or a pecuniary advantage as a result of or in connection with the commission of the offense, whereas the benefit itself is the value of the property so obtained (CJA 1990 Sections 1(4) and (5)). Issuing a confiscation order is at the Court's discretion, but such order can only be made on a written application of the prosecutor. The Court will assess the benefit of the criminal conduct and order the offender to pay a sum equal to that benefit, or an amount the court estimates to be realizable at the time of the order (CJA 1990 Section 1(6)). If payment is not forthcoming the High Court may then, on application made by or with the consent of the AG appoint and empower a receiver to realize any realizable property. CJA 1990 Section 4 gives detailed instructions on how realizable property has to be assessed, but basically it has to be understood as any property held by the defendant at the time of the order, together with the value of all gifts (including transfers for a significantly low value) he has made after the commission of the offense, but minus the debts resulting from priority obligations.

Drugs

217. The confiscation regime in the context of drug offenses is quite similar to that of CJA 1990. DTA 1996 also provides for the possibility of confiscation of the benefits upon conviction for drug trafficking, on application of the prosecutor. The rules on the assessment of the benefits and payment or realization of the confiscated amount are no different from those of CJA 1990, except that under certain conditions any property transferred to the offender within the period of six years before the institution of the criminal proceedings should be taken into account (S4(3)(a)(ii).

218. In all instances non-compliance with the confiscation orders can be sanctioned by imprisonment for a term to be determined by the court, with a maximum of 10 years.

Terrorism

219. ATCA 2003 Section 16 provides for the possibility of making forfeiture orders upon conviction of the defendant for terrorism offenses (ATCA Sections 7 to 10). The use of different terminology in the case of forfeiture (vis-à-vis the confiscation provisions) is explained by the fact that the order does not relate to a sum equivalent to the illegally gained benefit but to the money and other property the offender possessed or controlled at the time of the offense (fund raising and money laundering offenses) with the intention to be used for terrorism purposes or where he had reasonable cause to suspect that it would be used for that purpose. Payments and rewards in connection with the terrorism offenses are also subject to forfeiture. The issuing of forfeiture orders is at the discretion of the Court, but does not require a prior application by the prosecutor. ATCA 2003 Schedule 2 provides further detail in respect of the implementation of forfeiture orders and provides for the appointment of a receiver to take possession of and realize any forfeited property.

Instrumentalities

General

220. The power to confiscate (or more precisely “forfeit”, as it relates to specific items) instrumentalities used or intended for use for criminal purposes is provided for in the Criminal Law Act 1981 Section 16. Any property (intended to be) used for or facilitating the commission of an offense by a person convicted of the offense, and which was in his possession or under his control at the time of his apprehension or the summons, can be forfeited by the court with an order depriving the offender of his rights in respect of that property. The property is then taken into the possession of the police, irrespective if it has been previously seized or not. Forfeiture of the instrumentalities of crime under this Act applies to all crimes, including drug trafficking and terrorism.

Drugs

221. Additionally, instrumentalities used in or intended to be used in drug offenses can also be forfeited according to the Misuse of Drugs Act 1976, Section 27, empowering the Court, upon conviction, to forfeit anything shown to relate to the drug offense, to be either destroyed or dealt with in such a manner as the court may order.

Terrorism

222. Beside the general regime of the Criminal Law Act 1981, forfeiture of terrorism related instrumentalities may also be captured under ATCA 2003 Sections 16(2)(b) and (3)(b), forfeiting all property intended to be used for terrorism purposes (including raising funds for and financing of terrorism).

Equivalent value

223. The confiscation regime of CJA 1990 and DTA 1996 is essentially equivalent value based by itself, as it provides for the payment of a sum that in principle reflects the value of the proceeds (“benefits”) of crime. The confiscation order is then executed on the assets (“realizable property”) of the offender, where it does not matter if they have any relation with the offense or not.

224. The ATCA 2003 forfeiture provisions specifically target money and other property that is related to the terrorism offense and in the possession or under the control of the offender when he committed the offense. As such the ATCA 2003 contains no reference to any specific equivalent value confiscation or forfeiture and none of the DTA 1996 or CJA 1990 value confiscation rules apply to the ATCA 2003 situations.

Proceeds of Crime Act 2008

Proceeds

225. One of the most important new provisions introduced with effect from October 22, 2008 by the POCA 2008 Part 1 is the civil recovery procedure, based on the balance of probability evidence rule with no requirement for a previous conviction. Property being or representing proceeds from unlawful conduct could be forfeited by the High Court. Cash being or representing criminal proceeds,

or intended to be used in unlawful conduct could be forfeited in civil proceedings before a Summary Court.

226. Part 2 of the POCA 2008 covers confiscation and restraint in respect of all other crimes, except those covered by ATCA 2003. POCA 2008 Section 66 deals with the making of a confiscation order and would provide for the Court to determine whether the defendant has a criminal lifestyle; if so, whether he has benefited from his general criminal conduct; if not, whether he has benefited from his particular criminal conduct. The court would then determine a recoverable amount and make a confiscation order requiring the defendant to pay that amount. POCA 2008 Sections 66–73 contain further provisions regarding confiscation orders including determination of the recoverable amount, determination of the defendant's benefit, and determination of the available amount. POCA 2008 Sections 74–78 deal with procedural matters in respect of confiscation orders. Sections 79–86 provide for reconsideration, 87–88 provide for where the defendant absconds, and 89 and 90 provide for variation and discharge of a confiscation order. Appeals are dealt with by Sections 91 and 92, enforcement provisions in Sections 93–95, and the appointment, powers, and procedure in respect of management and enforcement receivers in Sections 103–117. POCA 2008 Section 215 provides for the making of secondary legislation which will enable confiscation orders made outside the IOM to be enforced in the IOM. The POCA 2008 is being brought into force in stages by Regulation and the existing provisions of DTA 1996 and CJA 1990 with regard to restraint and confiscation are being repealed.[13] The previous legislation continues to be used, however, until the new secondary legislation has been brought into force, thus ensuring a seamless transition. August 1, 2009 is the effective date for all remaining provisions of the POCA 2008.

Instrumentalities

227. The POCA 2008 does not deal with the forfeiture of the instrumentalities. The existing legislation (CLA 1981) will continue to apply. Also the specific legislation dealing with confiscation and forfeiture relating to terrorism will not be affected.

Confiscation of Property Derived from Proceeds of Crime (c. 3.1.1 applying c. 3.1):

228. As noted, confiscation under CJA 1990 and DTA 1996 is value based. The criminal proceeds are not subject to confiscation as such but, in calculating the total value of the benefits the offender gained from his criminal conduct, the Court will take into account all benefits derived directly or indirectly therefrom, which would include substitute assets, investment yields and other profits. It does not matter if the proceeds are held by the offender or by a third party. If no voluntary payment follows, the Court may appoint a receiver to execute the order on the offender's realizable property. "Realizable property" is defined in both Acts as "any property held by the defendant and any property held by a person to whom the defendant has directly or indirectly made a gift caught by this Act".

229. Proceeds of FT offenses, subject to forfeiture under ATCA 2003 Section 16, are defined in Section 6 as property wholly or partly and directly or indirectly representing the proceeds of terrorism

[13] The authorities expect to have the secondary legislation in place by late 2009.

related activity. The definition also covers payments and other rewards and would consequently cover all immediate and derived benefits.

230. Forfeiture of instrumentalities of (whatever) crime relates to identified objects, whether or not the property of the offender.

231. As for the rights of the bona fide third party, this is addressed in the analysis in this report of Recommendation 3.

Proceeds of Crime Act 2008:

232. The definition of criminal proceeds in the civil recovery part of the POCA 2008 (Section 3) is not specific. Property represents criminal proceeds if "obtained by or in return for the conduct", which does not make clear whether indirect proceeds are covered. The assessment of the benefit the offender acquired from the criminal lifestyle and the specific offense, however, comprises the value of all property which the Court considers the defendant has acquired as a benefit of crime. Such benefit is consequently not limited to the direct proceeds.

Provisional Measures to Prevent Dealing in Property subject to Confiscation (c. 3.2):

233. At the investigation stage the police have a general power of seizure of items or other property based on establishing reasonable grounds that they are the product of crime ("obtained in consequence of the commission of an offense") or have an evidentiary value (PPPA 1998 Section 22). Criminal proceeds could fall under both categories, especially if materially present in the form of cash. Police seizure of assets unrelated to the offense under investigation (equivalent value seizure) is not possible under the PPPA 1998.

General

234. Conservatory measures to preserve the assets subject to a confiscation order and to prevent their dissipation are found in CJA 1990 Sections 6 and 7 ("restraint orders"). Such an order is issued by the High Court prohibiting any person from dealing with any realizable property, subject to such conditions and exceptions as may be specified in the order. Restraint orders can however only be issued if criminal proceedings have been instituted against the defendant for an offense to which CJA 1990 applies. The confiscation proceedings may have not been concluded and either a confiscation order has been made or the court expects a confiscation order may be made.

Drug Trafficking

235. Restraint orders according to of DTA1996 Sections 25 and 26 follow the same line. Again, proceedings must have been instituted against the defendant for a drug trafficking offense, and confiscation proceedings have not been concluded and either a confiscation order has been made or the court expects a confiscation order may be made. Restraint orders can also be issued to take into account new elements; such as a change in the level of assets available to the defendant (Sections 13 to 16 and 19).

Terrorism financing

236. ATCA 2003 Schedule 3, part 2 contains a special procedure for seizure and detention of "terrorist cash", which extends to any financial instrument convertible into cash. The seizure can be effectuated by an "authorized officer" (customs, police) for 48 hours, after which an order of the High Bailiff is required to detain the cash for a longer period (three months to two years). Seizure during an investigation and of other terrorism related items as "evidence" can be effectuated under the relevant provisions of the PPPA 1998. Restraint orders can be issued under the rule of ATCA 2003 Schedule 2.5 (1) and (2) of the, provided criminal proceedings or criminal investigations have been initiated.

Equivalent value seizure

237. Seizure of assets unrelated to the offense is adequately covered by the restraint orders under CJA 1990 and DTA 1996, as this is made in preparation of a value based confiscation of realizable property, where no relation with the offense is required. It is less clear if equivalent value conservatory measures are available under ATCA 2003.

Proceeds of Crime Act 2008

238. POCA 2008 Section 97, in force from August 1, 2009, empowers the Court to make an order (a "restraint order") prohibiting any specified person from dealing with any realizable property held by that person and may apply to all realizable property held by a specified person, whether the property is described in the order or not, and to realizable property held by a specified person, being property transferred to him after the making of the order. The restraint order may be made subject to exceptions and conditions such as allowing for reasonable living and legal expenses, but differs from the existing legislation in disallowing provision for any legal expenses in connection with the offense or offenses for which the restraint order is sought and are incurred by the defendant or by the recipient of a tainted gift. The Court may exercise these powers provided any of the conditions specified in POCA 2008 Section 96 are satisfied. These conditions would be less onerous on the prosecution than the current requirements and allow a restraint order to be made once an investigation has been started rather than requiring proceedings to be instituted and that there is reasonable cause to believe that the alleged offender has benefited from his criminal conduct.

Ex Parte Application for Provisional Measures (c. 3.3) :

239. Both the current and new legislation in this area allow the initial application to freeze or seize property subject to confiscation to be made ex-parte. Applications for such orders, whether under the DTA 1996 or the CJA 1990 are made ex-parte by the prosecutor to a Deemster in chambers and once the order is made, notice of the order is made to persons affected by the order. As for ATCA 2003, Schedule 2.5 (4) allows the application to be made "in private without notice".

240. These provisions are mirrored by those in POCA 2008 Section 98.

Identification and Tracing of Property subject to Confiscation (c. 3.4):

241. A first and important role in the detection of suspected criminal proceeds is played by the FCU/FIU as receiving agency of the suspicious transaction reports by the industry under the AML/CFT rules.

242. At the investigation stage the police have several options:

- they can request the court to issue a production order pursuant to DTA 1996 Section 52 or CJA 1990 Section 17J requiring the person who holds the required information to produce it to a constable. If necessary the police can immediately apply for a search warrant.

- they can use the means provided in the PPPA 1998 (Sections 11 and 12, Schedule 1) and seek authorization from a judge to enter and search premises based on reasonable grounds for believing that a serious arrestable offense (which would include terrorism financing - see Schedule 2 of the PPPA 1998) has been committed and there is material on the premises which is likely to be of substantial value to the investigation of the offense.

243. A special procedure is used in cases of "serious or complex fraud", which is interpreted as covering all forms of dishonest behavior generating illegal benefits. Money laundering activity would fit in with that concept. CJA 1990 Section 24 empowers the AG to require from any person he has reason to believe has relevant information to attend before him and answer questions and furnish information with respect to any matter relevant to the information. This procedure does in principle not require a court intervention, but confers a discretionary power on the AG which is subject to judicial review (based on the criterion of reasonableness).

Proceeds of Crime Act 2008

244. POCA Part 4 has provisions that duplicate some and extend the provisions of DTA 1996 and CJA 1990 with regard to production orders, allowing production orders to be obtained in civil recovery as well as criminal confiscation investigations. POCA 2008 also contains additional powers that provide for search and seizure warrants, disclosure orders, customer information orders and account monitoring orders. However, the provisions of CJA 1990 Section 24 and PPPA 1998 have not been amended.

Protection of Bona Fide Third Parties (c. 3.5):

CJA 1990 and the DTA 1996

245. The procedure for assessing the value of realizable property takes into account the rights of creditors and of bona fide third parties by defining the "amount that might be realized" as the total value of property less the value of any obligations having priority and the value of that property as the market value of that property less the value of any other person's interest in that property (DTA Sections 6 and 7; CJA 1990 Section 4). Provision is also made for bona fide third parties to make representation to the court where a court has been asked to empower a receiver to enforce a charge or realize realizable property (DTA 1996 Section 29(8); CJA 1990 Section 10(8)). In restraint orders third parties affected by the restraint may make application to discharge or vary the restraint order (DTA 1996 Section 26(10) and CJA 1990 Section 7(7)).

246. ATCA Section 16(7) provides for innocent third party protection in the context of forfeiture orders, giving any interested third person the opportunity to be heard by the Court before the order is issued.

247. Forfeiture of instrumentalities under the CLA 1981 can be challenged before the Court by third parties under CLA 1981 Sections 16(4)(b).

248. In addition, there is always the general right of any person who feels wronged by confiscation or forfeiture measures to apply at any time to the High Court with a Petition of Doleance in order to obtain a judicial review.

POCA 2008

249. The POCA 2008 mirrors the provisions of the above legislation in respect of the rights of secured creditors. This provision is found in POCA Section 69 which states: "For the purposes of deciding the recoverable amount, the available amount is the aggregate of the total of the values (at the time the confiscation order is made) of all the free property then held by the defendant minus the total amount payable in pursuance of obligations which then have priority." Obligations are defined as preferential debts as specified in the Preferential Payments Act 1908. There are no corresponding provisions for debts which do not constitute preferential debts. When application is made to the court to confer powers on a receiver (for example to realize property) bona fide third parties' rights would be further safeguarded by the provisions of POCA 2008 Section 106(8) which states "The court must not confer the power mentioned in subsection (2)(b) or (c) in respect of property or exercise the power conferred on it by subsection (6) in respect of property, unless it gives persons holding interests in the property a reasonable opportunity to make representations to it." With regard to restraint, POCA 2008 Section 98(2)(b) provides that any person affected by a restraint order may apply to vary or discharge the order and any such person may appeal such an order to the Staff of Government Division (Appeal Court) pursuant to Section 99(2)(b).)

Power to Void Actions (c. 3.6):

250. In general, actions that are intended to willfully obstruct effective confiscation or forfeiture of criminal proceeds in whatever form constitute criminal offenses that amount to (aiding and abetting) money laundering and as such they give cause to prosecution. Any such actions would be illegal, so any such contracts or agreements are not taken into account in confiscation/forfeiture decisions. Moreover, in the context of the proceedings surrounding the realization of property by a receiver, the Court has wide powers to void any action that would undermine the value of the realizable property.

Analysis:

251. With the exception of the issues raised below; the IOM legal framework underpinning the seizure and confiscation system related to proceeds of crime is generally solid and comprehensive. The (similar) relevant provisions of CJA 1990 and DTA 1996 and, since October 22, 2008, POCA 2008 adequately provide for a value-based confiscation regime capturing in principle any benefit that the offender may have gained as a result of his criminal conduct. The benefit assessment procedure followed by the court is quite detailed and takes into account all factors necessary to come to a fair

estimation. The provisions of ATCA 2003 also appropriately focus on the deprivation of the assets related to FT.

252. There are however some issues that need review in respect of compliance with the international standards:

- the deficiencies identified with the criminalization of ML and FT may also affect the criminal conviction-based confiscation and forfeiture; and

- the "corpus delicti" confiscation of the assets laundered is untested and its application doubtful. It is understood that proving money laundering does not require a conviction of the predicate offense. However there is an issue of jurisdiction: the criminal conduct the Court has to judge is the money laundering activity itself and the confiscation of the benefits of that conduct, which is not the same as the benefits gained from the commission of the predicate offense(s). The jurisdiction of the Court does not extend to the predicate criminality, and consequently the authority of the Court to pronounce itself on the benefits of that conduct is subject to challenge.

253. Equivalent value seizure appears not to be fully covered in all circumstances. Restraint orders pursuant to CJA 1990 Section 6 and DTA 1996 Section 25 can only be issued when proceedings have been instituted against the defendant, leaving him the opportunity to dispose of his assets as soon as he is alerted to any investigative action, to ensure they would no longer be available as realizable property. This deficiency is remedied by POCA 2008 Section 96, with effect from August 1, 2009.

254. The IMF's 2002/03 AML/CFT assessment pointed out that confiscation of assets of equivalent value in connection with the FT was not covered in the IOM. The issue remains unresolved. Assets and proceeds related to FT are subject to forfeiture, which requires that the money and other property, representing wholly or partly and directly or indirectly the proceeds of the offense (ATCA 2003 Section 6 (2)(a)), be connected with the offense. Arguably it might not be necessary for the assets still to be available when the forfeiture order is issued, the requirement being only that the money and property was in the possession or under the control of the offender at the time of the offense. On the other hand there is a second condition in ATCA 2003 Section 16 that the assets are supposed to be used for the purposes of terrorism, imposing need to establish a concrete link between the assets and the FT offense.

255. This difficulty extends also to the issue of equivalent value seizure under ATCA 2003. Although the implementation procedure for the forfeiture orders reflects the same approach as the confiscation procedure, including restraint of property in preparation of a forfeiture order, ATCA 2003 Schedule 2.3(3) appears to confirm the requirement that the assets that are the object of the forfeiture order must be shown to have a specific connection to the offense, insofar as this shields the receiver from liability for any actions "in relation to property which is not forfeited property". If the receiver would be entitled to execute the order against any property of the offender, it would seem that such protection would be unnecessary.

Effectiveness:

256. The available statistical data covering the period between 1997 and 2003 show an uneven but reasonable number (113, ranging from two to 44 per year) of drug related confiscation orders. According to partial statistics for 2008 (up to June) seven confiscation orders were issued. Very noticeable in all cases is the difference between the assessed benefit and the amount actually recovered: no confiscation order has been fully or even substantially realized. The highest percentage is typically around 30 percent (with one exception of some 50 percent), the lowest some 0.01 percent. Although this reflects the universal challenge faced by law enforcement in terms of effective recovery of criminal assets , it indicates that efforts need to be increased. An important element is the need for timely immobilization or freezing of the assets so that they remain available for recovery. The introduction of civil recovery under POCA 2008 effective August 1, 2009, may prove useful in increasing effectiveness in this area.

257. The statistics kept in respect of the (domestic) restraints and confiscations are partial and insufficient to allow a comprehensive assessment of the performance of the recovery system.

258. The IOM seizure and confiscation legislative framework is generally adequate and reflects a clear awareness of the legislator of the importance of depriving criminals of their illegal assets. The authorities need to reinforce the legal framework to address the following issues in order to enhance effectiveness:

- the deficiencies in respect of the scope of the ML and FT offenses may affect the quality of the criminal confiscation regime;

- the possibility of confiscating the assets laundered in a stand-alone money laundering case is subject to challenge in the absence of case law or other authoritative source, though UK precedent may be helpful; and

- the undue restriction that equivalent value seizure is possible only after formal proceedings have been instituted.

2.3.2. Recommendations and Comments

- The law should be amended to address the deficiencies affecting the scope of the ML and FT offenses and thereby also improve the quality of the criminal confiscation regime.

- The law should be amended to:
  - allow equivalent value seizure at any stage of the investigation; and
  - address in ATCA 2003 the issue of equivalent value confiscation in the context of FT-related assets.

- Case law should be developed on stand-alone money laundering confiscations.

- The authorities should address the low effectiveness of the current asset recovery measures, particularly by focusing on the timely tracing and immobilization of recoverable or realizable assets

2.3.3. Compliance with Recommendation 3

	Rating	Summary of factors underlying rating
R.3	**PC**	• Deficiencies in ML and FT criminalization impact on the scope of criminal confiscation. • Confiscation of laundered assets might not succeed in stand-alone ML cases • At the time of the assessment, no equivalent value seizure possible before start of the proceedings. • For FT, barriers to application of equivalent value confiscation and seizure. • Overall effectiveness of confiscation measures needs to be improved.

2.4. Freezing of funds used for terrorist financing (SR.III)

2.4.1. Description and Analysis

Legal Framework:

259. Specific legislation on freezing suspected terrorist assets is found in the Al-Qa'ida and Taliban (United Nations Measures) (Isle of Man) Order 2002 (SI 2002 N° 259), the Terrorism (United Nations Measures) (Isle of Man) Order 2001 (SI 2001 No. 3364), and the European Communities (Terrorism Measures) Order 2002 (SD 111/02) and the European Communities (Al-Qaida and Taliban Sanctions) (Application) Order 2002 (SD 444/02).

260. Other legal measures against terrorism related assets, including terrorism financing, are found in ATCA 2003. The Act provides for both criminal and administrative measures aimed at restraining such assets in whatever form. The criminal seizure and forfeiture provisions cover all law enforcement actions in the investigating and judicial phase and are commented upon above. The administrative freezing measures taken by the Treasury under ATCA Sections 50 to 55 are more of a preventive, pre-investigative nature, and fall under the scope of SRIII.

Freezing Assets under UNSCR 1267 (c. III.1):

261. The UNSCR 1267 is enforced in the IOM through the Al-Qa'ida and Taliban (United Nations Measures) (Isle of Man) Order 2002 [SI 2002 N° 259], an Order-in-Council made in the UK under the United Nations Act 1946 (an Act of Parliament), extended to the IOM (Section 1(3)). Besides prohibiting the supply or delivering of goods ("restricted goods") to persons designated by the UNSCR 1267 Sanctions Committee, it makes it an offense to make any funds available to or for the benefit of a designated person. The Order further provides for the freezing of funds where the Treasury has reasonable grounds to suspect that they are in any way held or under the control of a designated person (Article.8).

262. In addition, the IOM also complies with the EC Council Regulation 881/2002 of May 27, 2002, giving effect to UNSCR 1267. This Regulation applies in the IOM, as part of the IOM's law, pursuant to the European Communities (Al-Qaida and Taliban Sanctions) (Application) Order 2002

[SD 444/02], using enabling powers found in the European Communities (Isle of Man) Act 1973 (an Act of Tynwald). EC Regulation 881/2002 contains a requirement for member states to implement measures to freeze the funds or other assets of designated persons.

Freezing Assets under S/Res/1373 (c. III.2):

263. The Terrorism (United Nations Measures) (Isle of Man) Order 2001 [SI 2001 No. 3364], an Order-in-Council made in the UK under the United Nations Act 1946 (an Act of Parliament), gives effect to UNSCR 1373. Article 1(4) extends the Order to the IOM. It installs a freezing regime, similar to the one giving effect to UNSCR 1267. Article 6 gives the (UK) Treasury the right to issue notices freezing any funds held by, for, or on behalf of a suspected terrorist or associated person.

264. In addition, the IOM also complies with the EC Council Regulation 2580/2001/EC of December 27, 2001, giving effect to UNSCR 1373. This Regulation applies in the IOM, as part of the IOM's law, pursuant to the European Communities (Terrorism Measures) Order 2002 [SD 111/02], using enabling powers found in the European Communities (Isle of Man) Act 1973 (an Act of Tynwald). Regulation 2580/2001 contains a requirement for member states to implement measures to freeze terrorist funds or other assets and to give effect to requests from other countries to freeze funds or other assets in their jurisdiction.

265. In general terms, ATCA 2003 Section 50 empowers the IOM Treasury to make a freezing order without application to the Court, when it reasonably believes that a foreign person or government presents a threat to the life or property of IOM and UK residents and to the IOM or UK economy. Such freezing order prohibits persons from making funds available to or for the benefit of a person or persons specified in the order, and can be issued to comply with the UNSCR 1267 and UNSCR 1373 obligations. A Protocol was drawn up by the Customs and Excise Division of the Treasury establishing a procedure whereby Section 50 freezing orders may be put in place. This Protocol was adopted in October 2008 and made the Sanctions Officer in the Customs and Excise Division responsible for coordinating consideration of the need for a Section 50 order.

266. The IOM Treasury has as yet not seen any reason to issue its own list of suspected terrorists, which would be drafted in consultation with the UK in any event. Any designation on the domestic list would assumedly also be based on information supplied by the FIU or other law enforcement bodies. The IOM's list of persons and entities subject to the freezing sanctions is kept in line with the UK designations.

Freezing Actions Taken by Other Countries (c. III.3):

267. The IOM has not incorporated foreign terrorist lists directly into its domestic freezing regime, other than through the EC Regulation and UK list. Foreign designations may be taken into account on a voluntary basis by the industry in their risk-based assessments and as a ground for suspicion to be reported to the FIU. An example of such list is the US OFAC list. The Customs and Excise Public Notices on the implementation of UNSCRs 1267 and 1373 also reminds the public and industry of their duty to report any suspicions of FT irrespective of whether or not the persons or organizations are listed.

268. There are no statutory provisions outlining the procedure to be followed when there is a formal request from another jurisdiction to incorporate their list of designations in the IOM freezing mechanism. The Terrorism (United Nations Measures) (Isle of Man) Order 2001 is silent in that respect, although it does make reference to the UNSCR 1373 in its explanatory note. The only other applicable legal provision is ATCA Section 50 empowering the Treasury, who may be considered to be the central and appropriate authority for the IOM to process such requests, to issue freezing orders if certain conditions are met. These conditions are rather restrictive, targeting only foreign persons and governments and excluding any listing if there is no threat to the IOM and UK economy or to the life or property of IOM or UK nationals or residents.

Extension of c. III.1-III.3 to funds or assets controlled by designated persons (c. III.4):

269. ATCA 2003 does not contain any detailed definition of funds, other than "money or other property" (throughout Part III on terrorist property) and "financial assets and economic benefits of any kind" (Section 51(6) in the context of freezing orders).

270. All special statutes covering the implementation of the freezing mechanism under the UN Resolutions and the EU Regulation are very specific and elaborate in defining the funds subject to freezing (Article 2 of the Al-Qa'ida and Taliban Order 2002, Article 2 of the Terrorism Order 2001 and Article 1 of the EC Regulations 2580/2001 and 881/2002 as applied in the IOM). Although quite detailed, none of them contain an express reference to assets that are "jointly" and "indirectly owned or controlled" by the designated persons. Derivatives of the funds (interests, dividends, etc.) are adequately covered.

Communication to the Financial Sector (c. III.5):

271. The UN, UK and EU lists are immediately disseminated by the IOM Customs and Excise by way of Public Notices and publication on the government and Customs and Excise websites. The lists and any changes are equally communicated through the Weekly Circular supplied by Customs and Excise to all of its own staff, and forwarded to the FSC, IPA, AG's Chambers, DHA, and other interested departments. The FSC and IPA also place the notices of changes in the lists on their websites. Public Notices are also available to the non-regulated entities and professions, such as the real estate agents and high value dealers.

272. The Public Notices contain details of the UN and EU measures concerned, and the legislation implementing and sanctioning them in the IOM. They also indicate the link to the relevant UK lists of designated persons and entities on the HM Treasury website. These are notified by news release published without delay via the IOM Government and Customs and Excise websites. Normally the news release is issued no later than the day following notification by HM Treasury of the changes.

Guidance to Financial Institutions (c. III.6):

273. Customs and Excises have provided guidance to the public in the Sanctions Notice 22 on the sanctions regime implementing UN Resolutions and the EC regulation. Dissemination to the industry is also done through the regulators' websites.

De-Listing Requests and Unfreezing Funds of De-Listed Persons (c. III.7):

274. The ATCA 2003 does not specifically provide for withdrawing or cancelling a freezing order issued under Section 50 but, as such freezing orders come within the definition of public documents, Section 28 of the Interpretation Act 1976 (which provides the power to make any public document) is relevant and includes the power to amend or revoke such public document. The Terrorism (United Nations Measures) (Isle of Man) Order 2001 Section 6(7), however, which also applies to domestic freezing lists in respect of suspected terrorist assets, provides for a formal challenge procedure against a direction of designation by the Treasury issued under the relevant order "in the same manner as the review of a direction under the Banking Act 1998" (since repealed and replaced effective August 1, 2008 by the FSA 2008, Section 32 of which provides for a Financial Services Tribunal to consider, inter alia, appeals against directions). However, until the coming into operation of rules made under Section 8 of the Tribunals Act 2006, the Financial Services Review Regulations 2001 shall apply to an appeal under Section 32 of the FSA 2008, and a reference to an application for the review of a decision by the FSC shall be construed as a reference to such an appeal and a reference to the Committee shall be construed as a reference to the Financial Services Tribunal (Article 8 of the Financial Services Act 2008 (Appointed Day) Order 2008).

275. This review request and procedure has not yet been applied in the IOM. In practice, as all IOM designation lists match the lists of designated persons in effect in the UK, all de-listing and unfreezing decisions in the UK will automatically be followed in the IOM.

276. Nothing is provided in terms of an intervention of the IOM authorities in a request to the UN Sanctions Committee to de-list and unfreeze assets frozen under UNSCR1267, or a similar request in relation to the EC Regulation. The specific de-listing mechanism of UNSCR 1730 (2006), providing for a designated person to make a request to the 1267 Committee through their State of residence or citizenship (beside the possibility of addressing a focal point at the UN), has not been considered by the IOM authorities. In practice, the IOM authorities liaise on any such action with the competent UK authorities.[14]

Unfreezing Procedures of Funds of Persons Inadvertently Affected by Freezing Mechanism (c. III.8):

277. There are no specific procedures or legislative provisions dealing with appeals or claims. There is, however, the general obligation of ATCA 2003 Section 52.2 instructing the Treasury to keep a freezing order under review. ATCA 2003 Schedule 9 also provides for the possibility of the freezing order containing provisions for awarding compensation to persons prejudiced by the order.

Access to frozen funds for expenses and other purposes (c. III.9):

278. Access can be provided to funds frozen under the UN Terrorism Order 2001 or the EC Regulations for humanitarian purposes and basic expenses if a license or authorization is granted by the Treasury, as provided for in the relevant orders (Terrorism (United Nations Measures) (Isle of

[14] Details of how to apply to the relevant UN department for delisting from UN-derived sanctions lists were added in March 2009 to all relevant Sanctions Notices issued by Customs and Excise.

Man) Order 2001 Article 14; EC Regulation 2580/2001, as applied in the IOM. Similar licenses can be granted under the freezing regime of the ATCA 2003 (Section 4 of Schedule 9).

279. There is no provision in respect of a possible access to assets frozen as a result of UNSCR 1267.

Review of Freezing Decisions (c. III.10):

280. As already noted, there are no specific remedies contained in ATCA 2003 with regard to an appeal procedure before a court. There is however the common law IOM remedy of Petition of Doleance to challenge the making by Treasury of such an order. A Petition of Doleance is a specific IOM remedy whereby an applicant would need to show that the Treasury had been unreasonable in the sense that no similar authority would reach the same conclusion in making such an order. The specific procedure involved in such a challenge would involve a petition to the High Court of Justice of the IOM. The court cannot overturn the decision nor substitute it with its own, but can send it back to the Treasury with guidance as to how to review the order. The court can also award damages.

Freezing, Seizing and Confiscation in Other Circumstances (applying c. 3.1-3.4 and 3.6 in R.3, c. III.11)

281. All penal conservatory and deprivation measures of seizure and confiscation or forfeiture that can be applied in respect of FT, (as discussed above in analyzing Recommendation 3), can also be used in relation with terrorist related assets in general. Reference is made to Part III of ATCA 2003 on terrorist property and related offenses and the forfeiture provisions. The deficiencies commented upon in the respective relevant sections of this report also apply here.

Protection of Rights of Third Parties (c. III.12):

282. There are several ways to protect bona fide third party rights. In the first place they can be taken into account in the freezing order itself made by the Treasury under ATCA 2003 Section 50. In particular, the licensing and authorization possibilities provided by the relevant UN and EC orders, and those provided in ATCA 2003 Schedule 9 particularly serve that purpose. Furthermore there is the possibility to apply for a review by the Review Committee. Finally the Petition of Doleance remedy may provide a means for redress.

Enforcing the Obligations under SR III (c. III.13):

283. Non-compliance with the freezing orders issued under the ATCA 2003 regime constitutes an offense according to Section 6 of Schedule 9 of the Act, punishable by custody up to two years. The UN Orders 2001 and 2002 provide for penalties that may run to seven years custody. Sanctions for non-compliance with the EC Regulations 2580/2001 and 881/2002 as applied in the IOM must be determined by each Member State (here including the IOM) according to Article 9 and Article 10 respectively. The European Communities (Terrorism Measures)(Enforcement) Regulations 2008 [SD 941/081] and the European Communities (Al-Qaida and Taliban Sanctions)(Enforcement) Regulations 2008 [SD 942/081], which came into effect on November 28, 2008, create the necessary offenses and penalties that provide that breaches of EC Regulations 2580/2001 and 881/2002 as applied in the IOM are punishable by custody for up to two years.

284. In addition, regulatory authorities such as the FSC, IPA, and DHA can apply their own range of sanctions, that could ultimately include revocation of a license. If the noncompliance could be interpreted as an act of supporting terrorism, criminal prosecution for FT could follow.

Analysis:

285. The implementation by the IOM of UNSCRs 1267 and 1373, as well as the 2001 and 2002 EC Regulations, is closely linked to that of the UK. All UK lists become automatically incorporated in the IOM freezing regime. The IOM has little or no input in the decisions taken in this context in respect of designations, delisting and unfreezing.

286. Although this has not yet been used in practice, the IOM has its own listing and freezing provisions in ATCA Part VII. The Act however contains a few accompanying measures, and is insufficient to ensure a comprehensive preventive, pre-investigative approach as required by the international standards. The Orders implementing the relevant UN Resolutions and the EC Regulations, together with already existing legal infrastructure, complete the freezing regime to a large extent.

287. ATCA Section 50 only applies to foreign persons or governments presenting a threat to the interests of the IOM or UK economy or the life or property of IOM or UK residents or nationals. It is not clear on what grounds these restrictions rest, particularly why it was deemed necessary to exclude IOM or UK suspects. Also the "economic interests" of the IOM or the UK that have to be threatened do not necessarily preclude an investment of terrorist related funds in the economy.

288. Based on the ATCA provisions, the specific UN Resolutions and EC Regulations Orders are the legal instruments that provide the basis in the IOM for an assets freezing regime, where the (UK) Treasury, more particularly the Customs and Excise, plays a key role in their implementation. Although the bulk of the international criteria are covered, some issues, mostly of a formal nature, still need to be addressed:

- No formal procedure is in place to receive and assess requests based on foreign freezing lists, as required by UNSCR 1373;
- The definition of "funds" subject to freezing does not cover the assets "jointly" or "indirectly" owned or controlled by the relevant persons;
- A procedure for considering de-listing or unfreezing requests is not provided for in the context of the EC Regulations;
- The possibility and procedure of access to UNSCR 1267 frozen funds for humanitarian purposes or basic expenses has not been provided for.

Effectiveness:

289. Assets of a designated person have been frozen in a bank account for an amount of GBP 72,924 in 2007, all in the same case. Another case was reported to the FCU in the form of an

STR, as there were no more assets to be frozen. These figures, though modest, indicate a certain level of awareness and compliance by the industry.

290. The obligations to introduce extra-ordinary freezing mechanisms, imposed by the supranational bodies, have received an adequate, if not a fully comprehensive, response from the IOM authorities. The system needs to be completed with adequate measures, most importantly in the area of protection of the basic interests and rights of persons affected by the listings. The other deficiencies noted are of a more technical nature.

2.4.2. Recommendations and Comments

- Put in place a formal procedure governing the receipt and assessment of requests based on foreign freezing lists, as required by UNSCR 1373.
- Amend the legal framework implementing the UN Resolutions and EC Regulations to expressly extend the definition of 'funds' subject to freezing to cover assets 'jointly' or 'indirectly' owned or controlled by the relevant persons.
- Amend the legal framework for the implementation of the EC Regulations to provide a procedure for considering requests for delisting or unfreezing.
- Provide for and publicize a clear procedure enabling access to UNSCR 1267 frozen funds for humanitarian purposes and to cover basic expenses.

2.4.3. Compliance with Special Recommendation III

	Rating	Summary of factors underlying rating
SR.III	**PC**	• No procedure in place to respond to and examine foreign freezing requests. • Definition of "funds" does not cover the 'jointly' and 'indirectly'. • No delisting or unfreezing procedure provided in the context of the EC Regulation lists. • No access provided to UNSCR 1267 frozen assets for humanitarian reasons and basic expenses.

Authorities

2.5. The Financial Intelligence Unit and its Functions (R.26)

2.5.1. Description and Analysis

Legal Framework:

291. The legal basis for the reporting regime is currently found in CJA 1990 Sections 17A(3) and 17B(5), DTA 1996 Sections 46(3), 47(5) and 48, and the ATCA 2003 Sections 11(2), 12, 13(2), 14 and 26, pursuant to which suspicions are to be reported to a 'constable'.15 In practice all such reports are directed to the FCU which, as noted, is part of the IOM Constabulary. As for the regulated sector, the AML Code 2008 Section 20(2)(f) specifically refers to a 'constable who is for the time being serving with the organization known as the Financial Crime Unit' as the person to whom the Money Laundering Reporting Officer of the covered entities ('regulated and relevant persons') should disclose suspicions of money laundering, which for the purposes of the Code includes also suspicions of terrorism financing (Section 2(1) Interpretation).

Establishment of FIU as National Centre (c. 26.1):

292. The FCU acts as the FIU for the IOM. It is a joint police/customs unit supported by civilian personnel. Its specific remit as a receiving and processing agency for ML and FT-related disclosures by the regulated and associated sector is formalized in the AML Code 2008. The FCU has no intermediary function, though the internal organization provides for a two-step process where the analytical section selectively disseminates information to the investigation section of the FCU. Disclosures made by anyone under the reporting rules of the CJA 1990 and DTA 1996 are to the FCU. FT related reports made under the ATCA 2003 provisions, referring to reports to be made to a 'constable', are also made to the FCU. The unit has been in operation since 1999 as a result of an organizational restructuring creating specialized sections within the Constabulary. Within its organization it has established a Financial Intelligence Unit (FIU) as a subsection of the unit, which acts as the first reception point of the disclosures and conducts an initial analysis of the information received.

293. The FCU is headed by a Strategic Board consisting of the Chief Constable, The AG and the Collector of Customs. The Strategic Board set out the strategic aims for the FCU, as follows:

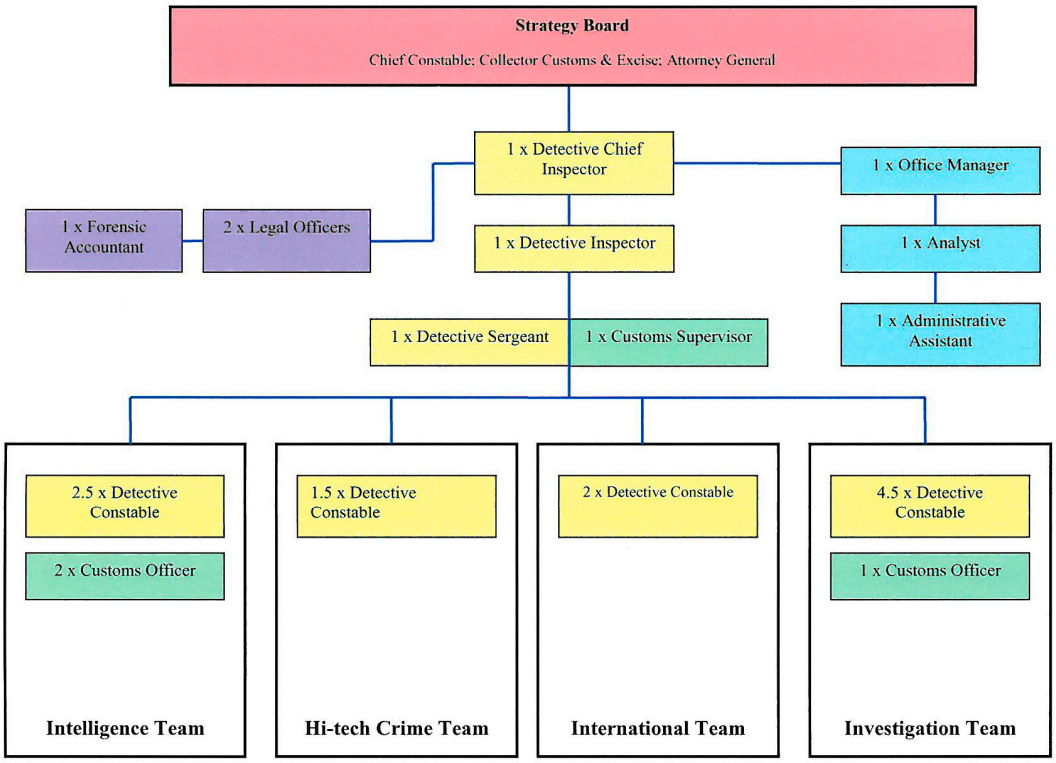
- To protect the Island's financial reputation and guard its financial community;
- To ensure that the Island is not seen as a safe haven for the laundering of money or the financing of terrorism; and

[15] Sections 142–144 of the POCA 2008, in force from August 1, 2009, will formally appoint (a constable or customs officer serving with) the Financial Crime Unit of the Isle of Man Constabulary as the reception point for 'authorized disclosures' (Section 154(1)). As for FT-related STRs, the relevant provisions of the ATCA 2003 would still apply, as the Act will only replaces the CJA 1990 and DTA 1996.

- To provide a one stop of professionals who ensure compliance with the law and with international standards predicated upon removing the profit from crime.

294. The following chart shows the organizational structure of the FCU.

FCU/FIU STRUCTURE AND RESOURCES



Guidelines to Financial Institutions on Reporting STR (c. 26.2):

295. The FCU encourages the reporting entities to use the disclosure form it has developed. The form is quite detailed (including identification, supporting documents, reasons for suspicion etc.) and, if correctly completed, covers all relevant information necessary to conduct an initial analysis and keep reliable statistics. Although not mandatory, the forms are widely used. The FSC's AML/CFT Handbook also contains guidance on STR disclosures and the forms to be used for reporting to the FCU. The FIU regularly communicates with the industry, including through seminars and other training sessions, reminding MLROs and other personnel of the proper use of reporting forms, the procedures to be followed and the quality expected. The reporting is still done manually: an on-line

system is being considered, but no concrete steps have been taken to automate the reporting system.16

Access to Information on Timely Basis by FIU (c. 26.3):

296. As a joint police/customs law enforcement unit, the FCU has full and direct access to an extensive range of intelligence databases, including all IOM police and customs registers, and can also access the main UK law enforcement databases. Administrative registers, such as VAT and tax data, are also directly available for consultation.

297. Financial information of a non-public nature is not readily available to the FCU and obtaining such data normally requires court approval if it is to be used in evidence. Collection of information held by financial institutions for intelligence purposes is possible only on an informal basis.

298. With regard to data access and usage, the terms of Section 25(3) of the Data Protection Act 2002 have to be observed. In all cases, information can be collected and used only for the purpose of prevention and detection of crime.

299. The FIU also utilizes internet-based search engines and databases to assist in its analysis and information gathering (data-mining) and consults commercial databases such as World Check, Experian, and C6.

Additional Information from Reporting Parties (c. 26.4):

300. As a law enforcement unit, the police and customs officers working within the FCU can use the information-gathering powers conferred on them by Sections 11–25 of the Police Powers and Procedures Act (PPPA), Sections 1(2), (3)(f), and 52–54a of DTA 1996 and Sections 17J, 24, and 25 of CJA 1990. With regard to FT, Sections 18, 24, 25, 31, 32 and Schedules 4, 5, and 6 of the ATCA 2003 provide relevant powers to FCU officers. As a rule, the use of these powers requires the approval of a magistrate or court, except in hot pursuit cases. These powers are, however, primarily intended to be used for investigative purposes and for collecting evidence. Non-compliance with the resulting production or similar orders can carry criminal sanctions.

301. When additional information is sought only for intelligence and/or analytical purposes, none of the above provisions apply and there are no direct powers provided to the FCU. The information is then supplied on a voluntary and informal basis, and any such request cannot be enforced. It appears however that the entities subject to the AML Code 2008 take a cooperative approach towards such requests, including queries made regarding beneficial ownership, not least to protect their reputations. The FCU informed the assessors that requests to reporting entities in general—whether or not to the original reporting party—to update or supplement information do not generally give rise to objections. Incomplete or deficient disclosures are returned to reporting entities for correction or proper completion.

---

[16] The POCA 2008 Sections 154(1)(b) and 155, in force from August 1, 2009, will make it obligatory to use the form to be prescribed by order of the Department of Home Affairs. It would make it an offense if the disclosure is made otherwise without a reasonable excuse.

Dissemination of Information (c. 26.5):

302. All STRs are analyzed by the FIU section within the FCU. The analysis mainly implies checking the databases at hand, making further enquiries to complete the picture, and comparison with ML and FT typologies. Exchange of information with counterpart FIUs and conferring with the IOM regulatory authorities are important elements of this process. If the FIU finds that a suspicion is grounded, the information is passed on to the investigators of the FCU.

303. Dissemination of the disclosed information is restricted. In principle it requires the consent of the person who supplied the information, except in the case of dissemination to domestic judicial, law enforcement, and regulatory authorities. FIU information can also be supplied to foreign law enforcement and prosecution authorities (CJA 1990 Sections 17H and 17I). As a practical arrangement the FIU has entered into Memoranda of Understanding to facilitate the exchange of information with domestic competent authorities, such as the FSC and the Tax authorities.

304. When disseminated, the information is at the discretion of the authorities to be used for the investigation and prosecution of any offense and is not restricted to ML or FT purposes.

Operational Independence (c. 26.6):

305. Although part of the IOM Constabulary, the FCU operates quite independently. This obviously does not preclude an effective interaction with other segments of the law enforcement community, but the structure and budget of the unit ensure a distinct degree of operational autonomy, even if the FCU personnel are seconded from their parent organizations and still work in partnership with them. The relative size of the FCU compared to its parent organizations and the investments made in the FCU show the importance of its role for the authorities. The operational independence and impartiality of the FCU is further protected by the multidisciplinary composition of its Strategic Board.

306. The FCU budget is separate from the police budget and is provided by the IOM Treasury to the DHA (which is responsible for the IOM Constabulary). The budget is further delegated and controlled by the Head of the FCU.

307. Operationally, the FCU works closely with the Constabulary, especially the Drug Trafficking Unit (DTU) in pro-active money laundering investigations involving drugs. It also has access to and liaises closely with other units within the Constabulary such as the Force Intelligence Bureau, Covert Operations, and the Constabulary's other investigative wings, including the Criminal Investigation Department.

Protection of Information Held by FIU (c. 26.7):

308. All FCU information is registered in the Government/Police secure computer server and can only be accessed by authorized personnel. Dissemination of information is covered by legislation (CJA 1990 Sections 17G–I, DTA 1996 Section 50, ATCA 2003 Sections 56–57, and the Data Protection Act), together with internal FCU policies and procedures. Police Officers employed within the unit are also covered by Police Disciplinary Regulations covering the improper disclosure of information. Customs officers and civil servants attached to the FCU are required to comply with

IOM Civil Service Regulations for disciplinary matters and the Official Secrets Act protecting the confidentiality of the information.

309. FIU-specific information, such as STRs 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 FCU/FIU.

Publication of Annual Reports (c. 26.8):

310. The FCU produces annual statistics on STR information which are published, pursuant to the provisions of the Police Act 1993, in the report of the Chief Constable of the IOM which is a publicly available document. The report can be viewed at www.gov.im/dha/police.

311. Typologies and trends are fed back to the industry through lectures and presentations given by the FCU and in joint presentations and seminars with the regulatory authorities. Advisory Notices are also produced and circulated to licenseholders on the latest threats, offenders, or trends. Typology information is communicated to the industry through the respective regulatory authorities, regular press releases, and lectures. Case feedback is also given as appropriate.

Membership of Egmont Group (c. 26.9):

312. The FIU has been an active member of the Egmont Group since 2000.

Egmont Principles of Exchange of Information Among FIUs (c. 26.10):

313. The FIU is fully committed to the Egmont Group and its Statement of Purpose and its Principles for Information Exchange. The FCU contributes to the running costs of the Egmont Group Secretariat, has access to the Egmont Secure Web, and attends the plenary sessions.

Adequacy of Resources to FIU (c. 30.1):

314. The structure chart below adequately shows the FCU's operational independence and autonomy. The FCU, which incorporates the FIU, has its own premises and is housed separately from the premises of the Police and Customs. The personnel are fenced from their parent organizations operational duties, enabling them to concentrate full time on their duties within the FCU/FIU. The Unit has its own vehicles at its disposal.

315. The current budget for the Unit including salaries and allowances is a sizeable percentage of the budget for the whole Constabulary. This budget is separate from the overall police budget and for the sole use of the Unit. It includes budgets for the training and development of staff, IT systems and equipment. It also includes travel and expense allowances. The Head of the Unit controls the proper use of the budgetary resources.

316. The FCU utilizes and has access to a wide variety of IT resources and datasets. It uses the Isle of Man Constabulary's IT system for its information management regarding STRs and uses other in-house IT systems, including analytical tools.

Integrity of FIU Authorities (c. 30.2):

317. All personnel are subject to vetting checks on employment and are security cleared to 'secret' level and are also subject to the Official Secrets Act as well as the legislative requirements regarding confidentiality.

318. FCU personnel are appropriately skilled and trained for their respective roles, maintain high professional standards, and undertake professional development courses and training courses throughout their careers. Training of personnel is considered by the FCU to be a priority, with a sizeable part of the budget focused on staff training and development.

Training for FIU Staff (c. 30.3):

319. Personnel recruited to the FCU are primarily from experienced detective backgrounds and have usually undergone criminal investigation training. They are subject to an application process which is evidence based, requiring them to show a competent level of skill in particular areas that are required for their role within the FCU. Personnel within the FIU receive additional training, including professional qualifications in compliance and anti-money laundering.

320. Some of the other courses undertaken by FCU/FIU staff include national terrorism financial investigation, national fraud courses, criminal investigation, suspect interviewing, check and credit fraud, financial investigators, bookkeeping, fraud examiners, high-tech courses including data analysis, and internet investigators.

Statistics (applying R.32 to FIU):

321. Detailed statistics are kept on the number of STRs, their sources, grounds for suspicion, nationality of the subjects, and other relevant information. The figures for the period 2004–2007 are set out in the analysis in this report of Recommendation 13. They do not indicate, however, the number of STRs that triggered an investigation. The number of investigations resulting from the reporting system was estimated at six cases over the last two years.

Analysis:

322. The formal foundations of the FCU as the central authority for the IOM to receive all suspicious transactions, subject them to an analytical process, and disseminate them to the competent authorities have not been embedded in specific primary legislation. The POCA 2008, in force from August 1, 2009, formally appoints the FCU as the FIU. This current lacuna has not prevented the FCU from organizing itself successfully in such way as to adequately implement the functions and responsibilities of an FIU.

323. The FCU has incorporated the specific duties and characteristics of an FIU by creating within its internal structure a special and distinct FIU team, so that a clear distinction can be made between the functions of the FCU as an intelligence unit and those as an investigative law enforcement body. This is especially important in the conduct of the external relationships of the FCU with foreign FIUs. This clear division of tasks is also operationally effective in that the FIU fulfills a selective and pre-investigative function in filtering out reports that do not warrant further investigation and adding value to the STR information received to prepare the case for further investigation, where the analysis

reveals sufficient indications. The separation between the intelligence and investigative functions of the FCU is equally important for developing a relationship of trust between law enforcement and the reporting entities, who can rely on the FIU to screen their reports for quality and relevance before deciding on a formal investigation. The relationship with the industry was observed during the assessment to be open and constructive.

324. The human and financial resources allocated to the FCU reflect the serious commitment of the IOM authorities to protecting the reputation of the financial center. The assessors noted the professional level of the FCU staff and their specific training and background in AML/CFT matters. The multidisciplinary approach of combining the expert knowledge of the police and customs officers, the analysts and the legal assistants at operational level, together with the balanced composition of the Strategic Board, are commendable. The informal basis on which the FIU collects additional information for analytical purposes offers flexibility and has been demonstrated to be effective in practice. However, such access to additional information depends on the goodwill and reputational awareness of the reporting entities; in the case of refusal of the informal request, the FCU would have to refer to the Courts and make use of its statutory investigative powers. As noted, the investigative processes are subject to formal requirements and procedures for the collection of evidence, and consequently are not generally available or suitable for use in the analytical stage. The FCU can and does share information successfully with its counterparts (as analyzed in this report for purposes of R. 40), as long as the case is still at the pre-investigative stage.

Effectiveness:

325. The statistics spanning a period of four years (2004/05–2007/08) show active reporting levels by the financial sector, ranging from 2,315 disclosures in 2004 to 1,555 in 2007/08. The numbers for 2008 are expected to remain at a similar level. The statistics show a marked decrease in STR reporting in 2006, but the number has stabilized since. The lower reporting level in 2006 was explained as being the result of an increased emphasis on quality. The FCU at the time took action against defensive reporting and rejected a number of them as insufficient and/or incomplete. The change in trend may also have been related to the timing of a South African tax amnesty which, coupled with the introduction of the EU Tax Savings Directive, caused a spike in reporting in the IOM in 2005. Some instances of non-compliance with reporting requirements have been reported to the regulatory authorities, which took appropriate action, serving as a warning to the sector.

326. The number of STRs resulting in an investigation (six in two years) is disappointingly low, especially taking into account that over the years only two prosecutions have been instituted in cases that originated with an STR. The proportionally modest amounts of effective asset recovery (as noted in the analysis for R3) also raises a question on the role the FIU can or should play in this area. Therefore, when measured in terms of concrete results from the overall system, effectiveness is an issue.

327. There may be several reasons explaining the low levels of cases and asset recovery, but one of the main factors is that, considering the offshore nature of the IOM financial industry, quite a number of disclosures relate to foreign predicate activity, with the proceeds coming to the IOM. Consequently the FCU/FIU is to a great extent dependant on the assistance received from its counterparts abroad, which is not always forthcoming or does not add much relevant information. Also relevant to an analysis of effectiveness is the positive impact of the frequent dissemination of

information by the FIU/FCU to the competent authorities of other jurisdictions, to assist in their analysis.

328. There are no indications of lack of timeliness or unreasonable delays in the processing of STRs due to internal structural factors. Delays are sometimes incurred where the FIU has to depend on external sources, such as its foreign counterparts. In this context, further steps could be taken and measures introduced to improve overall effectiveness, particularly as regard asset recovery where the assets have not yet been removed from the IOM. One possibility would be to endow the FCU/FIU with the power to freeze transactions; another is the requirement for prior consent of the FCU/FIU to release funds that are the subject of an STR that will be introduced on the coming into force of the POCA 2008. The prerequisite for improved effectiveness remains, however, the timely reporting by the sector itself regarding which some questions are raised in the analysis of Recommendation 13.

329. As noted, there is a weakness in the information gathering capacity of the FCU when acting as an FIU. The FIU should, according to the FATF standard, have direct or indirect access to financial and other additional information to adequately perform its functions. In the IOM, the direct process at FIU level is informal and voluntary. Access to such information could be available through a court application but this is an investigative measure that will normally only be considered by the judge if the case is at a sufficiently high evidentiary stage. Although rather theoretical at the time of the assessment as the FCU informed the assessors that no refusal has yet been encountered, the informal nature of the current access to additional information could be open to challenge and affect the information gathering capacity of the FIU for analytical purposes. Therefore, consideration should be given to providing for a formal (additional) information gathering process at FIU level.

330. Overall, the FCU/FIU is adequately performing its role as a key player in the AML/CFT system. It has developed a relation of trust and openness with the financial sector, which is also an important factor explaining the acceptable volume of STRs. Everything is in place to ensure that the STRs are appropriately dealt with in a focused and professional manner. The clear separation between the intelligence and the investigative side of the handling of the reports is particularly significant.

331. By contrast, the low number of STRs that result in investigations, and ultimately in a prosecution, raises a serious effectiveness issue that needs to be addressed. The fact that the FCU/FIU makes relevant information readily available to foreign counterparts is a positive factor, but does not sufficiently address the low level of results from the domestic system. This is a challenge for the authorities as a whole and not just for the FCU/FIU. Nonetheless the FCU/FIU should examine possible new ways to enhance its performance in terms of cases for investigation and asset recovery. The planned increase in numbers of qualified FCU/FIU staff (already approved by the authorities) is a good step in that direction, as is the proposed requirement for prior FCU/FIU consent for release of funds that is part of the POCA 2008 innovations.

2.5.2. Recommendations and Comments

- The authorities should supplement the current informal arrangement by providing formally for access by the FIU to additional information held by covered entities, for use in its analytical work.

- The FCU and other authorities should implement steps to improve the effectiveness of the reporting system to support an increase in the number of investigations and (potentially) prosecutions and in funds and other assets frozen.

2.5.3. Compliance with Recommendation 26

	Rating	Summary of factors relevant to s.2.5 underlying overall rating
R.26	**LC**	• No formal power of access to additional information for FIU analytical purposes. • Limited effectiveness of the overall reporting system, as reflected in low numbers of domestic FCU investigations.

2.6. Law enforcement, prosecution and other competent authorities—the framework for the investigation and prosecution of offenses, and for confiscation and freezing (R.27, & 28)

2.6.1. Description and Analysis

Legal Framework:

332. The legal framework for the investigation and prosecution of ML and FT offenses and for related seizure and confiscation measures is provided by the CJA 1990 (non-drug crimes related ML), the DTA 1996 (drug related ML), the ATCA 2003 (FT and related ML). The Police Powers and Procedures Act (PPPA) 1998 covers their investigative powers and the conservatory measures taken during a police investigation.

Designation of Authorities ML/FT Investigations (c. 27.1):

333. The following law enforcement authorities are, generally or particularly, charged with the investigation of ML/FT offenses:

334. The IOM Constabulary is primarily responsible for the investigation of all offenses. Specialized units within the Constabulary deal with specific criminality areas, such as drug trafficking. All cases related to ML and FT are allocated to the investigation branch of the FCU. As noted, the inherent powers of a constable in respect of stop and search, entry, search and seizure, arrest, and detention are set out in the PPPA 1998. Specific powers are conferred on police officers by the CJA 1990 and DTA 1996 or are supported by a court order.

335. Officers of Customs and Excise Division are empowered by provisions of the Customs and Excise Management Act 1986 to administer, investigate, and enforce the various provisions of the customs and excise legislation and other legislation in respect of “assigned matters”. Assigned matters include drug trafficking and money laundering related to Customs offenses, (such as indirect tax, VAT carousels, and smuggling), and enforcement of UN and EU sanctions, particularly in relation to terrorism assets (section 184(1) of the Customs and Excise Management Act 1986).

336. Effectiveness considerations resulted in the establishment of the FCU as a joint police and customs department, comprising officers of the Constabulary and officers of Customs and Excise

Division of Treasury. The unit is responsible for the investigation of financial crime, particularly ML and FT. Officers of the FCU who are officers of the IOM Constabulary have the powers of a constable in respect of all offenses; officers of the FCU who are officers of the Customs and Excise Division have the powers of a Customs Officer in respect of assigned matters. A new Section 77A was inserted into the PPPA 1998 by the POCA 2008 with effect from October 22, 2008, allowing customs officers at the FCU, when authorized in writing by the AG, to have the powers of a constable in relation to their work at the FCU. The AG signed the necessary authority on November 12, 2008 for officers working at, or available to work at, the FCU to have the powers of a constable in relation to their work at the FCU.

337. Prosecution is primarily in the hands of the AG and his staff of prosecutors (five at the time of the assessment but increased to seven subsequently). Distinction is made between summary proceedings where the prosecution may be handled by a police officer[17] and proceedings on information for the more serious cases, which would normally include ML and FT (such as the cases that ended up in a conviction), that are dealt with by prosecutors.

338. The AG's Chambers provides legal advice and expert assistance in all financial investigations including ML and FT. There are currently two full time dedicated legal officers supporting the FCU. The AG also advises the Chief Minister in relation to decisions relating to the interception of communications (Interception of Communication Act 1988).

Ability to Postpone / Waive Arrest of Suspects or Seizure of Property (c. 27.2):

339. The PPPA 1998 provides a power to arrest and seize. The power is not a duty and the exercise of that power can be deferred, postponed, or waived for the purposes of identifying persons involved in criminal activities or for evidence gathering. Deferring the arrest of suspected persons or seizure of criminal items or assets is a common law enforcement practice aiming at maximum effectiveness. It is the responsibility of the officer in charge of the investigation to decide on arrests, which may entail allowing an illegal situation to continue in a controlled way. Postponement of arrest to achieve maximum results is not exceptional in drug trafficking cases.

Additional Element—Ability to Use Special Investigative Techniques (c. 27.3); Additional Element—Use of Special Investigative Techniques for ML/FT Techniques (c. 27.4):

340. Measures are in place providing law enforcement or prosecution authorities with an adequate legal basis for the use of a wide range of special investigative techniques when conducting investigations of ML or FT. Key legislation in this area includes the provisions of the Interception of Communications Act 1988 Sections 2–7 which allow the interception of communications on obtaining a warrant signed by the Chief Minister and the detailed provisions of the Regulation of Surveillance etc. Act 2006 which provide for the authorization of surveillance and human intelligence sources, including directed and intrusive surveillance and covert human intelligence sources (undercover operations). Controlled delivery of the proceeds of crime or funds intended for use in terrorism is not prohibited by IOM legislation and is therefore permitted, as is the deferment of arrest,

[17] This arrangement was altered subsequent to the assessment. With effect from June 22, 2009, prosecutions are handled only by lawyers from the AG's chambers.

provided that the decision to do so is reasonable in all the circumstances. These powers have not been used yet in ML or FT cases.

341. The provisions of CJA 1990 Section 17A and 17B offer a degree of protection to employees of financial institutions who co-operate with the police when techniques such as controlled delivery are used. These provisions allow a person to assist another to retain the benefit of criminal conduct or acquire or use the proceeds of criminal conduct, provided he obtains the consent of a constable to do so.

342. Officers of the FCU have undergone training as financial investigators and specialize in investigating the proceeds of crime. They, together with legal officers of the AG's Chambers focus on the investigation, seizure, freezing, and confiscation of the proceeds of crime.

Ability to Compel Production of and Searches for Documents and Information (c. 28.1):

343. In respect of CDD and other relevant information held by financial and other entities subject to AML/CFT requirements, there are several legal provisions giving police officers the power, through application to the courts, to obtain such information and search premises at any stage of the investigation under DTA 1996 Sections 1(2) , (3)(f), and 52-54a , together with CJA 1990 Sections 17J, 24, and 25. Also the provisions of PPPA 1998 Sections 11–25 on searches and seizure apply.

344. With regard to FT, ATCA 2003 Sections 18, 24, 25, 31, 32 and Schedules 4, 5, and 6 provide for account monitoring orders, search warrants, and financial information orders, issued by the appropriate Court at the application of a constable.

345. CJA 1990 Sections 24 and 25 give the AG special powers to obtain evidence without a court order in respect of serious or complex fraud, wherever committed. The AG has the power to require the production of evidence and it is an offense to refuse to comply.

346. The powers outlined above are also available to Customs Officers who are included within the definition of 'Constables' within the Acts.

Power to Take Witnesses' Statement (c. 28.2):

347. All law enforcement officers are entitled and have the power to take down statements of witnesses. This common authority is inherent to the function of a police or customs officer, and is imbedded in the general principles of criminal law and procedure.

348. Adequacy of Resources to Law Enforcement and Other AML/CFT Investigative or Prosecutorial Agencies (c. 30.1):

349. The Police is operationally independent and no instances of undue political influence or interference are on record. The Constabulary is a department covered by the DHA which also looks after the fire brigade, probation, civil defense, and prison. The IOM Constabulary comprises 293 full time officers and is as a whole committed to fight criminality, including ML and FT. Section 4(3) of the Police Act 1993 specifically prevents any interference with the discipline and disposition of the Police Force.

350. The AG's Chambers comprised five prosecutors at the time of the assessment. With the anticipated coming into force of the POCA 2008 and the expected increase of the workload as a consequence of the introduction of the civil recovery regime, two additional prosecutors were subsequently recruited.

Integrity of Competent Authorities (c. 30.2):

351. Personnel recruited by the Constabulary are put through a stringent recruitment process involving several interviews, background checks, and team building exercises. Once recruited they are subject to a 10 week period of training in law and other skills followed by a period of tutoring by an experienced officer. The officer then has to serve a minimum of two years probation which, when passed, allows them to apply to be assigned to specialized departments.

Training for Competent Authorities (c. 30.3):

352. The Drug Trafficking Unit has received training in AML/CFT from the FCU and has also trained financial investigators for drug profit confiscation enquiries. It is an operational policy for any drug investigation to give attention to the financial aspects.

353. Training has been given regarding the POCA 2008 to enable all officers to be aware of the legislative powers to prevent/detect and deter ML and other relevant provisions. This has been done by placing the subject on sergeants' development courses, involving direct training input from a member of the FCU. Further briefings have been provided to specialized departments such as the Drug Trafficking Unit.

Statistics (applying R.32):

354. Statistics are kept at the FCU in respect of the number of investigations and prosecutions in relation of ML where persons have been arrested. The FCU informed the assessors that two prosecutions to date have been based on cases where the investigation was triggered by an STR.

355. Overall, the law enforcement authorities are adequately resourced and trained. They have a sufficient legal arsenal at their disposal to conduct investigations. In respect of the effectiveness of the ML and FT investigations, the effectiveness issues raised in relation with the FCU/FIU are also relevant to an analysis of law enforcement aspects.

356. As for the judicial side, the limited number of successful prosecutions points to a lack of effectiveness of the overall system. There are some legal deficiencies, as noted under Recommendations 1 and 2 above, but these are not the decisive factor. More effort and emphasis is needed on the development of case law on stand-alone money laundering, in situations where the prosecution is not so dependent on the need to collect evidence outside its jurisdiction.

2.6.2. Recommendations and Comments

- The authorities should implement steps to improve effectiveness by seeking to increase the number of investigations and prosecutions pursued domestically.

2.6.3. Compliance with Recommendations 27 & 28

	Rating	Summary of factors relevant to s.2.6 underlying overall rating
R.27	**LC**	• Limited effectiveness of the system as reflected in low numbers of domestic investigations and prosecutions.
R.28	**C**	

2.7. Cross Border Declaration or Disclosure (SR.IX)

2.7.1. Description and Analysis

Legal Framework:

357. The IOM introduced secondary legislation (European Communities (Cash Controls) (Application) Order 2008) ('the Order') to apply a cross-border cash control regime to comply with EC Regulation 1889/2005 of the European Parliament and of the Council of October 26, 2005 ('the EC Regulation'). The Order came into effect on June 1 2008. Penalties for non-compliance with the Order are provided for by the Cash Controls (Penalties) Regulations 2008.

358. The Proceeds of Crime Act 2008 (Appointed Day)(No.1) Order 2008 [SD 743/08] brought Part 8 of the Act into operation, inserting the new Part VA into the Customs and Excise Management Act 1986, and replacing the Order with effect from October 22, 2008. The Customs and Excise (Cash Declaration and Disclosure) Order 2008 [SD 745/08] prescribed the form for the declaration of cash entering or leaving the IOM with effect from November 1, 2008. The new cash declaration regime came into operation on November 1, 2008, with the revised Public Notice and new form made available at the airport and sea terminal and on the Customs and Excise website.

359. Mechanisms to Monitor Cross-border Physical Transportation of Currency (c. IX.1):

360. The IOM opted for a declaration system, in line with the regime in force at the external borders of the EU, which imposes an obligation on persons importing into or exporting from the IOM cash and bearer-negotiable instruments to a value of EUR10,000 or more to make a report to Customs and Excise. Import and exports by post, courier (fast parcel/packet) services and freight are, in principle, covered by the same legal provisions as apply for import and export by travelers (Section 15 of the Post Office Act 1993; Section 76 Customs and Excise Management Act 1986). It should be noted that movements of goods by mail between the UK and IOM are not regarded as imports or exports under the customs legislation in both jurisdictions, but are treated as "domestic". Interference with mail moving between the UK and IOM is only permitted by court order, unless the packet has been detained by the Post Office under its own powers because it contains something which Post Office regulations say cannot be sent by post (including drugs, noxious substances, explosives etc.), or if it contains contraband that got into the UK by evasion of customs controls there (e.g. tobacco smuggled into the UK from a third country and then mailed on to the IOM).

361. The declaration regime applies to the physical transportation of:

- currency in any denomination,
- bearer-negotiable instruments (such as travelers' checks),
- negotiable instruments (such as money orders, checks and promissory notes) that are either in bearer form, endorsed without restriction, made out to a fictitious payee or otherwise in a form such that title passes upon delivery, and
- incomplete negotiable instruments (that are signed, but with the payee's name omitted).

362. At the time of the on-site visit two such declarations had been made (importation of GBP30,300 and GBP15,000, respectively, in cash). Three more declarations have been received subsequently (two outgoing and one incoming – none of then gave rise to suspicions).

Request Information on Origin and Use of Currency (c. IX.2):

363. As a general rule, Section 79(4) of the Customs and Excise Management Act 1986 allows a customs officer to put questions to anyone entering or leaving the IOM in all circumstances. This would include any questions on the origin of the money when there are any doubts regarding its legality. Failure to declare or filing an incomplete or incorrect report could raise such suspicions. With effect from October 22, 2008, Part VA of the Customs and Excise Management Act 1986 provides explicit powers for customs officers to question persons and to proceed to search them, their luggage, and their means of transportation.

364. The Proceeds of Crime Act 2008 (Appointed Day)(No.1) Order 2008 [SD 743/08] brought Part 8 of the Act into operation, inserting the new Part VA into the Customs and Excise Management Act 1986, with effect from October 22, 2008. It provides enhanced powers for customs officers, with explicit powers to question persons and to proceed to search them, their luggage, and their means of transportation. Although the European Communities (Cash Controls) (Application) Order 2008 was already interpreted as covering sea and air cargo, now the scope of the declaration obligation is explicitly extended to situations where cash is not actually being 'carried' with or on the person but is contained in goods, or in a vehicle, ship, or aircraft (Section 76 Customs and Excise Management Act 1986).

Restraint of Currency (c. IX.3):

365. Filing a false or incomplete declaration does not in itself warrant the restraint or seizure of the cash. If however there are reasons to believe that the cash might be the proceeds of crime or might be used for criminal purposes the cash may be seized under DTA 1996 Section 39, or CJA 1990 Section 23A (which becomes POCA2008 Section 46 with effect from August 1, 2009). This is a general power for law enforcement officers, irrespective of the amount.

366. CJA 1990 Section 76G, introduced by the POCA 2008 (Schedule 5) with effect from October 22, 2008, now specifically authorizes Customs to seize the cash, if more than (the equivalent of) EUR10,000 is being carried, and:

- the person has refused to make a disclosure;

- the officer reasonably suspects the disclosure is false in a material particular (i.e., excluding minor inaccuracies);
- evidence has been required from the person but not produced, or does not support the information given by the person; or
- the officer reasonably suspects that the cash is property obtained through unlawful conduct or is intended for use in money laundering, other unlawful conduct or terrorism.

Retention of Information of Currency and Identification Data by Authorities when appropriate (c. IX.4):

367. All information contained in the declarations is stored in the Customs database. Sections 174B and C of the Customs and Excise Management Act cover the interaction between the Customs and other law enforcement authorities in respect of information access, allowing mutual information exchange for law enforcement purposes subject to the provisions of the Data Protection Act 2002.

Access of Information to FIU (c. IX.5):

368. On the basis of the above provisions a copy of the declarations and details of any false declaration or suspicions are to be forwarded to the FCU. There is no formal and specific provision making such communication to the FCU mandatory; the customs officers at the FCU automatically have access to the declaration registered on the Customs database.

Domestic Cooperation between Customs, Immigration and Related Authorities (c. IX.6):

369. Coordination for law enforcement purposes between the relevant authorities is a matter of common practice, particularly enhanced by the comparatively small size of the IOM's law enforcement community, who operate in a close working environment with established points of contact for the exchange of information. As already pointed out, the Customs and Excise Management Act provides the formal legal basis for the cooperation in all matters related to the cross-border cash transportation regime. Coordination between the Customs[18] and Police is structured within the FCU, which would deal with all AML/CFT issues arising from the declaration system.

International Cooperation between Competent Authorities relating to Cross-border Physical Transportation of Currency (c. IX.7):

370. Section 174B of Customs and Excise Management Act 1986 also specifically refers to international cooperation, where it states that Customs and Excise is able to cooperate with other authorities in exchanging information or documents for broad criminal investigation or proceedings purposes, whether in the IOM or elsewhere.

371. In addition, the IOM Customs participate in the global information exchange network based on bilateral and multilateral Customs agreements. Due to the IOM's special relationship with the EU

[18] Customs and Excise also assists the Immigration Officers, and its frontline staff are authorized to act as immigration officers–being able to deal with out-of-hours flights, pleasure craft, and non-scheduled air and sea movements..

and Customs membership of the Customs Union, many of the EC regulations governing exchange of information on customs, excise, and VAT fraud are applicable in the IOM, along with other relevant Conventions such as the Nairobi Convention, the 1998 Vienna Convention, the Naples II Convention, and the CIS Convention.

Sanctions for Making False Declarations / Disclosures (applying c. 17.1-17.4 in R.17, c. IX.8

372. Non-compliance with the European Communities (Cash Controls) (Application) Order 2008 is penalized according to the Cash Controls (Penalties) Regulations 2008, replaced since October 22, 2008 by Schedule 5 of the POCA 2008.

373. Part VA (Sections 76A to 76H) was inserted into the Customs and Excise Management Act 1986 through the POCA 2008 (Schedule 5). Any 'refusal' to declare or disclose and any untrue declaration or disclosure will be penalized:

1) on summary conviction, by custody for a term not exceeding six months or by a fine not exceeding GBP5,000, or both; or

2) on conviction on information, by custody for a term not exceeding two years or by a fine, or both.

The 'refusal' should be understood as any kind of willful non-declaration, excluding negligence. In addition Section 76G provides for the possibility to seize any cash 'to which the refusal, declaration, disclosure….relates', irrespective of the amount.

374. Disclosures were required under the interim regime only from 'natural' persons, the same requirement as set out in the EC Regulation and applying in EU Member States.

Sanctions for Cross-border Physical Transportation of Currency for Purposes of ML or TF (applying c. 17.1-17.4 in R.17, c. IX.9):

375. Depending on the evidentiary value of the available information and elements, the ML and FT-related criminal procedure and code provisions will apply, and criminal charges can be brought against the person also within the context of the cross-border declaration regime.

Confiscation of Currency Related to ML/FT (applying c. 3.1-3.6 in R.3, c. IX.10):

376. Police and customs officers are empowered to seize cash, when persons are entering or leaving the IOM, where there are reasonable grounds to suspect it may be linked to crime (CJA 1990 Section 23A and DTA 1996 Section 39), including ML and FT. With the coming into operation of Part 1 of the POCA 2008 effective October 22, 2008, the scope of these powers has been extended to any situation or place where an officer is lawfully present anywhere in the IOM. In addition to the forfeiture and conviction measures provided for in the CJA and ATCA, a forfeiture decision can also be issued by the High Bailiff, if so warranted.

Confiscation of Currency Pursuant to UNSCRs (applying c. III.1-III.10 in SR III, c. IX.11):

377. Persons crossing the border with funds subject to the UNSCR 1267 and 1373 sanctions, or attempting to do so, are in breach of the legislation imposing those sanctions. Furthermore, the cash would be liable to seizure by police or customs under CJA 1990 Section 23A or ATCA 2003 Schedule 3, and potentially to confiscation depending on the evidentiary value of the available elements.

Notification of Foreign Agency of Unusual Movement of Precious Metal and Stones (c. IX.12):

378. Customs and Excise has available a wide array of provisions allowing it to exchange information with other countries and territories which they use in practice in dealing with an unusual or suspicious movement of high value goods. As well as applicable EU legislation permitting mutual assistance in customs matters with EU Member States (Council Regulation (EC) No. 515/97), and EU-third country customs mutual assistance agreements (which have application in the IOM under Protocol 3 to the UK's Act of Accession to the European Community), Section 174B, Customs and Excise Management Act 1986 deals, inter alia, with the disclosure of information to any agency anywhere for the purposes of:

> '(a) any criminal investigation whatever which is being or may be carried out, whether in the IOM or elsewhere;
>
> (b) any criminal proceedings whatever which have been or may be initiated, whether in the IOM or elsewhere;
>
> (c) initiating or bringing to an end any such investigation or proceedings, or of facilitating a determination of whether it or they should be initiated or brought to an end.'

Safeguards for Proper Use of Information (c. IX.13):

379. The holding, recording and dissemination of information is subject to the IOM's Data Protection Act 2002. This Act transposed the EC Data Protection Directive 95/46/EC. Access is only permitted for law enforcement purposes to the relevant authorities (Sections 174 B and C Customs and Excises Management Act 1986).

Statistics (applying R.32):

380. No computerized database has been established by Customs and Excise to date. At present, the statistics can be maintained manually, considering the limited number of declarations (five since June 1, 2008). The declarations are also recorded in the FCU/FIU database.

Analysis

381. In regard to cash transportation by mail, there is an issue of compliance with the SR.IX in that the current requirements do not extend to mail between the UK and the IOM, which may also undermine the effectiveness of the measures now in place.

382. While the cash declaration system in place at the borders of the IOM largely corresponds with the international standard, a small reservation related to the proportionality and dissuasiveness of the sanctions in comparison with other jurisdictions where the non-declaration, as such, can be sanctioned by seizure. Part VA of the Customs and Excise Management Act 1986 addressed this issue with effect from October 22, 2008 and provides for a new regime for cash declarations with stiffer sanctions, including seizure. Although not a point of substance, the assessors noted that the IOM declaration threshold of more than EUR10,000 is not technically in full compliance with the EU Regulations which refer to amounts of EUR10,000 or more.

2.7.2. Recommendations and Comments

- The cross-border control requirements should be extended to cover cash transportation by mail between the UK and the IOM.

2.7.3. Compliance with Special Recommendation IX

	Rating	Summary of factors relevant to s.2.7 underlying overall rating
SR.IX	**LC**	• The cross-border control regime does not cover cash transportation by mail between the UK and the IOM.

3. PREVENTIVE MEASURES —FINANCIAL INSTITUTIONS

Customer Due Diligence & Record Keeping

3.1. Risk of money laundering or terrorist financing

383. As noted in section 1 of this report and as acknowledged by the IOM authorities, some characteristics of the IOM financial system point to an elevated potential for abuse for ML or FT purposes. While in reality not all of this business is high-risk, much of it would fall within the range of categories suggested by the FATF Methodology as examples of higher-risk business, including as follows:

- The authorities indicated that more than 90 percent of the customer relationships and of financial service business conducted are on a non face-to-face basis for nonresidents of the IOM[19];
- In many cases the business relationship is established through introducers (IOM or foreign) that are subject to varying levels of regulation, depending on their origin. Subject to certain controls, IOM financial institutions are permitted to rely on the introducers to conduct CDD on their behalf;[20]
- Financial services provided include private banking facilities for non-residents; and
- The use of legal persons and arrangements such as trusts is prevalent, both as asset-holding vehicles and as part of more complex structures that have the potential to create an additional challenge for IOM financial institutions in fulfilling the requirement to accurately identify the customer and the ultimate beneficial owner or controller.

384. The above characteristics are among those taken into account in the analysis in sections 3 and 4 of this report, in assessing whether the IOM's AML/CFT regime provides adequately for enhanced due diligence for higher-risk customers and business and is being implemented effectively.

385. The IOM authorities informed the assessors that they have not sought to exclude any of the categories of financial business or types of institutions set out in the FATF Methodology from the scope of the AML/CFT provisions on the basis that they might represent a proven low risk of ML or FT. However, as noted in section 4 of this report and in the analysis of Recommendations 33 and 34, an effective de minimis threshold is applied in determining whether a person provides relevant services 'by way of business'[21] and thus falls to be licensed under the FSA 2008 and subject to

[19] While deposit statistics indicate that approximately 30 percent of bank deposits in the IOM are from resident sources, much of this business relates to deposits placed with banks by IOM fiduciaries which are acting on behalf of nonresident beneficial owners.

[20] The IPA advised that such permission is rarely used in practice by (life) insurance businesses.

[21] 'By way of business' is not a defined term in the legislation

monitoring of their compliance with the AML/CFT requirements. The exemption allows for trust and corporate service providers to conduct an otherwise regulated activity without a license if the level of activity is below a certain threshold.

386. As described in section 1 of this report, the IOM authorities have recently formalized the availability to financial institutions of an overall risk-based approach, for which purpose the financial institutions are required to conduct a detailed risk analysis. This provides financial institutions with some discretion for prioritization in the day-to-day implementation of the detailed CDD requirements. The requirements and their implementation are analyzed in detail in sections 3 and 4 of this report. Where appropriate to particular assessment criteria, reference is included as to whether or not the available risk-based approach is consistent with the applicable FATF Recommendations.

Legal framework

387. Since the last IMF AML/CFT assessment of the IOM in 2002/3 the authorities have revised and expanded significantly the legislative basis for AML/CFT measures both in response to the recommendations of the 2003 assessment report and to reflect the substantial changes in the FATF Recommendations, as revised in 2004. The current provisions are outlined below and analyzed in detail in sections 3 and 4 of this report.

388. Under the 2004 Assessment Methodology for the FATF Recommendations, an asterisk applied to a criterion indicates that the relevant measures must be in law or regulation. To qualify as such, the requirements must have been issued or authorized by a legislative body and be shown to impose mandatory, enforceable, and sanctionable requirements. This is relevant to many of the requirements under Recommendation 5, as well as all of Recommendations 10 and 13. The requirements in respect of the remaining FATF Recommendations must, at a minimum, be specified in 'other enforceable means', defined by the FATF methodology as measures issued by a competent authority and shown to be mandatory, enforceable, and sanctionable. The following paragraphs set out the laws, regulations, and, as applicable, other enforceable means taken into account for the purposes of this assessment.

389. The main legislative foundation for customer due diligence (CDD) and other AML/CFT preventive measures in the IOM is the CJA 1990, Section 17 of which defines ML offenses, tipping-off offenses, and the offense of not reporting suspicious transactions. The Act also deals with confidentiality and provides exceptions to enable disclosure in certain restricted circumstances. CJA 1990 Section 17F also gives power to the DHA to issue codes for the purposes of preventing and detecting ML (whether relating to the proceeds of criminal conduct, drug trafficking, or otherwise).

390. CJA 1990 specifies that codes issued pursuant to Section 17F shall be laid before Tynwald, which has the power to annul the proposed code at either of its next two sittings. Having regard, therefore, to the power granted by the parliamentary body (in primary legislation) to the DHA to issue codes for ML purposes, combined with the passive parliamentary approval procedure here described, the assessors are satisfied that a code issued by the DHA under CJA 1990 Section 17F constitutes secondary legislation and is within the scope of the FATF definition of 'law and regulation'.

391. Pursuant to CJA 1990 Section 17F the DHA had issued AML Code 2007, which contained detailed provisions addressing many–though not all–of the elements of the FATF Recommendations. AML Code 2007 was revoked on the coming into force of AML Code 2008 on December 18, 2008. AML Code 2008 applies to persons conducting relevant business as listed in Schedule 1 to the Code, which includes a wide range of financial business relating, in particular, to financial institutions and DNFBPs. By comparison with the definition of 'financial institutions' in the Glossary of the FATF methodology, the IOM list defining the scope of the AML Code 2008 (as with its predecessor) is partially activity-based and partially institution-category specific. While the assessors cannot conclude definitively that the scope of coverage in the IOM is fully in line with the FATF definition, no material omissions from coverage were identified during the assessment. The assessors note that while most forms of lending and leasing business are defined as being within the scope of the IOM requirements, implementation focuses in practice on the categories of financial institutions covered by the Core Principles. While the IOM list also includes 'the business of the Post Office in respect of any activity undertaken on behalf of the National Savings Bank' (UK), the assessors were informed by the FSC that this refers to a previous agency arrangement and is no longer relevant as the Post Office no longer collects any funds or application forms under this arrangement. The analysis in section 3 below will focus on the following categories of financial institutions which operate in the IOM:

Category of financial institution:[22]	**Licensed**[23] **under:**	**Regulatory Authority:**
Banks/deposit takers	FSA 2008	FSC
Building Societies/other societies[24]	FSA 2008	FSC
Investment businesses and services to collective investment schemes[25]	FSA 2008	FSC
Money services businesses[26]	FSA 2008	FSC

[22] Another potential category is credit unions. Although provided for in legislation, none has ever been formed.

[23] FSA 2008 is, inter alia, a consolidation of the provisions of previous sectoral legislation. However, all previous licenses required reissue for purposes of the FSA 2008.

[24] There are three building society authorizations in issue, all of them relating to the IOM operations of UK building societies.

[25] They conduct business in the IOM under the following categories: stockbrokers, asset managers for collective investment schemes, financial advisers, managers and administrators of collective investment schemes. Their activities, respectively defined as class 2 and 3 in the Regulated Activities Order 2008, correspond to the following in the definition in the FATF methodology: trading in money market instruments, foreign exchange, exchange, interest rate and index instruments, commodity futures trading, participation in securities issues and the provision of financial services related to such issues, individual and collective portfolio management, safekeeping and administration of cash or liquid securities on behalf of other persons and otherwise investing, administrating or managing funds or money on behalf of other persons.

[26] Responsibility for authorizing money services businesses (MSB), including bureaux de change passed to the FSC on the coming into force of the FSA 2008 on August 1, 2008. The MSBs were previously registered by Customs and Excise. The FSC began to apply a supervisory regime (including AML/CFT measures) to the MSBs with effect from January 1, 2009.

Insurance business	IA 2008[27]	IPA
Insurance intermediaries	IA 2008	IPA
Moneylenders	Moneylenders Act 1991	Office of Fair Trading

392. As outlined above, CJA 1990 Section 17F provides the DHA with the power to issue Codes to prevent and detect money laundering, including money laundering relating to the benefits of proceeds of criminal conduct, of drug trafficking or otherwise. The scope of the CJA 1990 and therefore the power of the DHA to issue Codes do not, however, expressly extend to terrorist financing as defined in the ATCA 2003. The authorities indicated that they considered FT to be validly within the scope of the power of the DHA under the CJA 1990 to issue codes 'whether in respect of the benefits or proceeds of criminal conduct…or otherwise', although the provision in question relates specifically to forms of money laundering. While the assessors did not consider this in itself to be a convincing legal basis, they took into account that the resultant secondary legislation (AML Code 2007 and its replacement the AML Code 2008) were both the subjects of a parliamentary process which provided an opportunity for parliament to annul the codes, should they object to the content; no such objection was raised. On that basis, it would not be reasonable to conclude that the interpretation of the scope of the codes to include FT was ultra vires as regards the powers of the DHA, given that the parliamentary process, by default, granted consent to the content of the codes. The codes were accepted, therefore, for purposes of this assessment as including FT, although the assessors recommended that the opportunity be sought by the authorities to provide a more explicit legal basis in primary legislation.

393. A very significant sub-set of the business covered by the CJA 1990 is within the regulatory ambit of the FSC pursuant to the provisions of FSA 2008 (which consolidated previous regulatory legislation, including the Banking Act 1998). Among the regulatory objectives of the FSC under FSA 2008 Section 2(2) is 'the reduction of financial crime' which is defined in the Act as 'any crime involving (a) fraud or dishonesty; (b) misconduct in, or misuse of information relating to, a financial market; or (c) handling the proceeds of crime or funds connected with terrorism'. This definition is significantly narrower than the full range of predicate offenses for ML and FT required to be covered under the FATF Recommendations but includes explicit coverage of FT.

394. As the functions of the FSC are to be exercised in a way that is compatible with its regulatory objectives (Section 2(1)), the inclusion of the reference in Section 2(2) to financial crime empowers the FSC to apply to the institutions it regulates a wide range of provisions relevant for AML/CFT purposes. FSA 2008 Section 18 provides that the FSC may make rules (referred to as the Rule Book) to, inter alia, give 'full effect to the regulatory objectives' of the FSC under the Act. The FSC is required to consult with the Treasury regarding the Rule Book (to comply with FSA 2008 Section 44(5)) and follow the Tynwald procedure set out in FSA 2008 Section 45, which involves laying the Rule Book before Tynwald as soon as practicable after it is made. Unless Tynwald approves the Rule Book within the next two sittings, it ceases to have effect. The FSC confirmed to the assessors that, at the time of the onsite visit, they had completed the entire Rule Book and brought Chapter 9 of the

[27] The Insurance Act 2008 came into force from December 1, 2008 and is largely a consolidation of previous insurance legislation, superseding the Insurance Act, 1986 (as amended by the Insurance Act, 2004) which contained the same licensing provisions.

Rule Book relating to AML/CFT into force for all licenseholders with effect from August 1, 2008, that the procedure outlined above was followed, and the whole Rule Book was voted on and adopted by Tynwald following the required motion and discussion in Tynwald. On the basis that the Rule Book was approved by a parliamentary body as outlined above and therefore constitutes secondary legislation, it is accepted for purposes of this assessment as meeting the FATF definition of 'law and regulation'. The remaining chapters of the Rule Book (of less relevance for purposes of this assessment) were brought into force for new licenseholders from August 1, 2008 and for existing licenseholders from January 1, 2009.

395. The FSC has also issued to the institutions it regulates an AML/CFT Handbook, which lists among its purposes to 'outline the regulatory powers which the FSC may exercise and to set out the FSC's requirements of licenseholders'. While the Handbook is presented as guidance, much of its language is mandatory in tone and it is regarded by financial institutions as the principal single-source reference of the AML/CFT requirements with which they must comply. The Handbook also explains the FSC's expectations for the application by the institutions of the risk-based approach. The cover page of the Handbook confirms that it is not a legal document and should not be relied upon in respect of points of law. On that basis, the FSC agreed with the assessors that it cannot be regarded for the purposes of this assessment as meeting the FATF criteria for 'other enforceable means'. Nonetheless, the Handbook contains useful supporting and explanatory material, including much of the detail needed for the day-to-day implementation of the requirements of the law, the AML Code, and the Rulebook. In that respect, the detailed assessment includes quotes from the Handbook as appropriate.

396. Given that the financial institutions regulated by the FSC appear to be subject in parallel to the requirements of the AML Code 2008 and the FSC's Rulebook, both of which are secondary legislation, a question could arise as to which takes legal precedence in cases where their provisions overlap. The assessors are not aware of any basis for determining which piece of secondary legislation would take precedence other than by decision of the Courts should a case come before them, which has not occurred to date. While the revisions contained in the AML Code 2008 remove almost all of the potential conflicts which could have arisen under its predecessor, the assessors recommend that the authorities conduct a further review to remove any residual potential for conflicts and bring the requirements into full consistency with each other and with the international standard. The same point may arise in relation to the AML/CFT provisions applicable to insurance business, as described below. However, the assessors note that the amendments introduced by the authorities shortly after the on-site visit have already addressed the material inconsistencies.

397. Insurance business is subject to IPA authorization and supervision. While covered by the AML Code 2008 in the same manner as FSC licenseholders, insurance businesses are also subject to a set of insurance-related AML/CFT requirements, which were updated shortly before the current assessment. The previous AML/CFT provisions (the Anti-Money Laundering Standards for Insurance Business, the most recent version of which was issued in March 2003) have been superseded with effect from September 1, 2008 by the:

- Insurance (Anti-Money Laundering) Regulations 2008 (IAMLR 2008);

  and in the case of long-term insurance business by the

- Guidance Notes on Anti-Money Laundering and Preventing the Financing of Terrorism – for Insurers (Long Term Business) (IGN 2008).[28]

398. In addition, much of the insurance legislation was superseded by the Insurance Act 2008 (IA 2008), for which Royal Assent was received and its provisions brought into effect on December 1, 2008, to consolidate most of the current legislative provisions. For purposes of this assessment, both the IA 1986 (as amended) and the IA 2008 which has superseded it have been taken into account. While the text of this report refers mainly to the provisions to the IA 2008, it should be borne in mind that they largely replicate the provisions in effect at the time of the on-site visit under the previous legislation.

399. Pursuant to Section 2 of the Insurance Act 2008 (IA 2008), the functions of the IPA are linked to a number of regulatory objectives which include 'the reduction in the extent to which it is possible for any insurance business to be used in connection with the commission of financial crime', which is defined by Section 52 IA 2008 to include 'handling the proceeds of crime or funds connected with terrorism'. In exercising its functions, Section 2(2) provides that the IPA shall have regard, inter alia, to 'the desirability of insurers being aware of the risk of their businesses being used in connection with the commission of financial crime'.

400. Section 50 IA 2008 provides that the IPA may issue regulations 'as it considers are necessary or desirable to carry [the] Act into effect'. Pursuant to Section 32 IA 1986, the IPA issued IAMLR 2008, Section 5 of which extended the scope of the Regulations to include countering the financing of terrorism. The legal basis for this inclusion of FT is provided by the definition in Section 50 IA 2008, as quoted above.

401. IAMLR 2008 is accepted as secondary legislation for the purposes of this assessment as it:

- was issued under a specific power granted in primary legislation to the IPA to issue regulations, including explicitly in relation to the prevention and detection of money laundering;

- was laid before Tynwald in line with the parliamentary procedure, under which Tynwald could have exercised the right to annul such regulations in accordance with Section 50(4) of the IA 2008 (passive approval process by a parliamentary body); and

- contains mandatory provisions, which are enforceable by the IPA and subject to the sanctions of the Insurance Acts.

402. IAMLR 2008 applies to insurers; other IPA-regulated entities such as insurance intermediaries and managers, registered scheme administrators, and scheme trustees are subject to the AML Code 2008.

[28] The IPA explained that, in their view, ML and FT risk exposure varies across the different segments of the insurance sector. The IPA's AML/CFT requirements are focused particularly on the international insurance business (within the scope of long-term business here referenced), where the perceived risk is highest.

403. As noted, the IPA has issued AML/CFT guidance notes (IGN 2008) for insurers undertaking long-term business, which also came into effect on September 1, 2008. Following careful consideration, the assessors determined that these guidance notes should be accepted as 'other enforceable means' (OEM) for the purposes of this assessment, on the following basis:

- IGN 2008 is issued pursuant to IA 1986 Section 24C (as inserted by Section 12 of the 2004 Amendment Act), superseded by Section 51 IA 2008, which provides that the IPA 'may issue Guidance Notes for the purpose of providing binding guidance with respect to…any matter in respect of which regulations may be made under this Act';

- IGN 2008 is stated to have been laid before Tynwald, although it is not evident that there is an applicable parliament procedure for such as document;

- IGN 2008 specifies that, 'while these are Guidance Notes, the requirements set out herein must be considered as a mandatory minimum' and they are stated in mandatory language;

- The guidance notes, being issued under explicit statutory powers of the IPA and linked to the requirements of the relevant primary and secondary legislation, are enforceable under the supervisory powers of the IPA; and

- Not to comply with them exposes the insurer to regulatory sanctions as set out under the Insurance Act, which provides an acceptable sanctioning basis for purposes of the February 2008 revision to the FATF Methodology. No sanctions had been applied at the time of the on-site visit, but that is to be expected as IGN 2008 had only been in effect at that time for a number of days.

404. The legal basis is summarized in the following table:

Summary of legal basis for AML/CFT measures for financial institutions:							
Position as at: December 18, 2008	**Issued by/ under**	**Institutions covered:**	**Scope includes AML and CFT?**	**Primary legislation**	**Secondary legislation**	**OEM**	**Guidance**
CJA 1990	Tynwald	All covered entities	AML only	**X**			
AML Code 2008	DHA/ CJA 1990 Laid before Tynwald	All covered entities	AML covered explicitly, CFT by interpretation[29]		**X**		

[29] Power to issue secondary legislation to include FT within its scope is considered by the authorities to be covered by the use of the words 'or otherwise' in the enabling provision of the CJA 1990. Tynwald raised no objection to the resultant Code 2007 or Code 2008.

FSC Rule Book	FSC / FSA 2008 Approved by Tynwald	All FSC licenseholders (banks, securities firms, funds, CSPs, TSPs)	AML and CFT		X		
FSC Handbook	FSC/ FSA 2008	All FSC licenseholders (banks, securities firms, funds, CSPs, TSPs)	AML and CFT				X
Insurance Act (IA 2008)	Tynwald	All insurance businesses	AML and CFT	X			
IPA Insurance Regulations (IAMLR 2008)	IPA/ IA 2008 Laid before Tynwald	Insurers[30]	AML and CFT		X		
IPA Insurance Guidance Notes	IPA/ IA 2008 Laid before Tynwald	Insurers (long-term business)	AML and CFT			X	

3.2. Customer due diligence, including enhanced or reduced measures (R.5 to 8)

3.2.1. Description and Analysis

Prohibition of Anonymous Accounts (c. 5.1):

405. While anonymous accounts and accounts in fictitious names are not prohibited in primary legislation in the IOM, they are effectively prohibited in secondary legislation, in either a direct or indirect manner.

406. AML Code 2008 does not explicitly prohibit anonymous accounts but paragraph 4(1) requires all persons conducting an activity in the financial sector to undertake identification and verification procedures on all applicants for business. The opening of an anonymous account would conflict with this requirement. For FSC-regulated entities, there is an express prohibition in the FSC Rule Book 2008 (Rule 9.3 (1)) pursuant to which a licenseholder must not maintain an anonymous account or an account in a fictitious name.

407. In respect of insurers regulated by the IPA, IAMLR 2008 Section 15 expressly prohibits the establishment or creation of anonymous bonds or contracts in fictitious names and any such business relationships in existence 'must be treated as high risk and subjected to enhanced due diligence and ongoing monitoring'. The IAMLR 2008 applies to insurers; other IPA-regulated entities such as

[30] Not including insurance intermediaries and managers, registered scheme administrators, and scheme trustees

insurance intermediaries, insurance managers, registered scheme administrators, and scheme trustees are subject to the AML Code 2008.

408. The regulatory authorities informed the assessors that no indication of the operation of anonymous accounts was found in the course of their onsite supervision. The financial institutions interviewed during the assessment indicated no knowledge of the operation of anonymous accounts in the IOM. The assessors noted, however, that the responses received did not entirely exclude the possibility that some old anonymous accounts might still exist. This possibility is also acknowledged in the above reference from the IAMLR 2008, which seeks to address the heightened risk arising from anonymous insurance bonds or contracts, should they be identified in existing business relationships.

409. The use of numbered accounts is not proscribed and there is no specific reference to them in primary legislation or in the AML Code 2008. For FSC-regulated entities, however, Rule 9.3(2) of the FSC Rule Book 2008 requires licenseholders that maintain numbered accounts to 'identify, and verify the identity of the customer' and maintain the account 'in such a way as to comply fully with the requirements of the Code' and the AML/CFT requirements of the FSC Rule Book 2008. The assessors found this approach to be consistent with Recommendation 5.

410. The financial institutions interviewed during the assessment indicated no knowledge of the operation of numbered accounts in the IOM. However, the FSC decided to make provision in the Rule Book for any numbered accounts which might be operating.

When is CDD required (c. 5.2):

5.2(a)

411. Consistent with the FATF Recommendations, the authorities opted to set out the requirement to undertake CDD measures in secondary legislation. Pursuant to AML Code 2008 paragraph 6, identification procedures apply to new business relationships. The Code stipulates that relevant persons (which includes all financial institutions) must identify the applicant for business before the business relationship is entered into or during the formation of this relationship 'but in any event as soon as reasonably practicable (taking into account the need not to interrupt the normal conduct of business where there is little risk of money laundering or terrorist financing occurring) after contact is first made' (paragraph 6(2)). AML Code 2008 paragraph 6(9) provides that, in the absence of satisfactory evidence of identity, the business relationship shall not proceed any further, the relevant person should terminate the relationship, and must consider whether to file an STR. The issue regarding the timing of identification is addressed further below. The establishment of new business relationships based on information received from business introducers or other third parties is addressed in the analysis of Recommendation 9.

412. AML Code 2008 paragraph 6(5) provides for a limited exception to the obligation to produce evidence of identity for new business relationships where the identity of the applicant and nature and intended purpose of the relationship are known to the financial institution and the applicant is regulated by the FSC or IPA under their regulatory legislation, or is an advocate or registered legal practitioner or an accountant carrying on business in or from the IOM subject to equivalent AML/CFT professional rules, or is conducting regulated business (as defined) in a country listed by the IOM authorities as having an acceptable AML/CFT regime. While this appears to be a wide set of

exceptions, the relief from the obligation to conduct CDD measures applies only to an applicant that meets the specified criteria and not to the customers of or business introduced by such an applicant (except in the case of intermediaries and, for example, fiduciary deposits).

413. For FSC-regulated entities, there is also an explicit requirement in the FSC Rule Book 2008 (Rule 9.6 (5)) that a licenseholder must not proceed with a business relationship unless specified CDD measures have been conducted, including identification and verification of identity. This would appear to have the potential to conflict with AML Code 2008 paragraph 6 which allows some leeway regarding the timing of CDD. However, Rule 9.5 of the FSC Rule Book 2008 allows the FSC-regulated entities to conduct CDD measures, including in respect of an applicant for business, 'on the basis of materiality and risk'.

414. In the case of insurance, IAMLR 2008 Section 8 permits the insurer to complete the required CDD measures 'as soon as reasonably practical' after receipt of an application to enter into a business relationship. In the event that the business relationship is utilized before CDD is completed, the insurer must apply measures to control the type and volume of transactions. IGN 2008 expands on the rationale and provides examples of transactions that might be conducted before CDD is completed and measurements to be taken in such circumstances. Pursuant to IAMLR 2008 Section 9(1) and IGN Section 2.5, in the absence of satisfactory evidence, the business relationship must not proceed.

415. For IPA regulated insurers, discretion regarding the timing of verification of identity is permitted, except for beneficiaries under a trust. Pursuant to IAMLR Section 12, for a beneficiary named or nominated under a life policy, such verification can be undertaken at or before the time of a payout of a claim or exercising of rights under the policy.

5.2(b)

416. With regard to occasional transactions, AML Code 2008 uses the term 'one-off transaction' which is defined in paragraph 2 of the Code as any transaction (other than an exempted one-off transaction) carried out by relevant persons other than in the course of an established business relationship. An 'exempted one-off transaction' is defined in the Code as a one-off transaction (whether a single transaction or a series of linked transactions) where the amount of the transaction or the aggregate of a series of linked transactions is less than:

- EUR3,000 (or the equivalent thereof) in the case of a transaction or series of linked transactions entered into in the course of bookmaking or casino businesses; or
- EUR15,000 (or the equivalent thereof) in any other case. (Code paragraph 2(1)).

417. For IPA-regulated insurers, under IAMLR 2008 Section 7, CDD requirements may be waived for contracts for which:

- the premium, payable in one installment, does not exceed GBP7,500;
- the regular premium payable in any calendar year does not exceed GBP2,500; or
- The contract does not have a maturity or surrender value, such as term life insurance.

418. In line with Recommendation 5, for all transactions outside the scope of these concessions, the regulated entity must undertake the same identification procedures as when entering into a new business relationship before a one-off transaction is entered into (AML Code 2008 paragraph 9). For insurers that avail of the above threshold concessions, CDD measures must be undertaken if a claim or return premium is greater than the monetary waiver thresholds (IAMLR 2008 Section 7(4)(5)).

419. Section 4.3 of the FSC Handbook provides further guidance regarding the interpretation of linked transactions, indicating that the FSC has no objection to the adoption of the previous UK standard of three months as the minimum acceptable monitoring period to determine whether a series of transactions has exceeded the applicable threshold for linked transactions.

5.2(c)

420. There is no provision in primary legislation, in the AML Code 2008, or the FSC Rule Book 2008 relating to wire transfers. The IOM authorities opted instead to implement European Regulation 1781/2006 on Wire Transfers by means of orders made by the Council of Ministers, which constitutes secondary legislation in the IOM: the "European Community (Wire Transfers Regulation) (Application) Order 2007", as amended by the "European Communities (Wire Transfers Regulation) (Application) (Amendment) Order 2007".

421. Payment service providers are required, before transferring funds, other than from an account, to verify the complete information on the payer on the basis of documents, data, or information obtained from a reliable and independent source, where the amount exceeds EUR1,000 (or the transaction is carried out in several operations that appear to be linked and together exceed EUR1,000). The exemption threshold does not apply where there is a suspicion of money laundering. (European Regulation (Application) Order, paragraph 5.4).

422. The measures applicable to wire transfers are compliant for purposes of Recommendation 5 and are analyzed in more detail later in this report when addressing SR.VII.

5.2(d)

423. Financial institutions are required pursuant to the AML Code 2008 to undertake CDD measures regardless of any available exemption if they know or suspect (or a suspicious pattern of behavior causes them to know or suspect) that the transaction is or may be related to money laundering when entering into a new business relationship or conducting a one-off transaction (paragraphs 6(8)(a) and (b), 9(8)(a) and (b), and 11(11)(a) and (b) AML Code 2008).

424. The application of this requirement to situations when financing of terrorism is known or suspected is based on the definition in the AML Code 2008 of 'money laundering requirements' which includes the requirements of ATCA 2003 Sections 7–11 and 14. As discussed elsewhere in the report, the power of the DHA to issue the Code under CJA 1990 Section 17F refers explicitly to preventing and detecting money laundering and, although accepted for purposes of this assessment that FT is also covered by extension, the assessors recommend that the authorities seek the opportunity for a more explicit legal basis. On balance, the assessors concluded that, in this respect, the IOM can be considered compliant with Recommendation 5.

425. For IPA-regulated insurers, simplified or reduced levels of CDD must not be applied where there is a suspicion of money laundering (IAMLR 2008 Section 13(3)) and IAMLR Section 5 extends this provision to FT. Pursuant to IGN 2008 5.3, CDD must also be undertaken upon surrender or maturity of a contract if there is suspicion of ML or FT

5.2(e)

426. AML Code 2008 paragraph 7(2)(f) requires customer due diligence procedures to be undertaken where a relevant person 'becomes aware of anything which causes the relevant person to doubt the veracity or adequacy of evidence of identity produced under paragraph 6(3)' of the Code. AML Code 2008 paragraph 7(2)(e) requires CDD procedures to be undertaken if 'the relevant person becomes aware of anything which causes the relevant person to doubt the identity of the person who, in relation to the formation of the business relationship, was the applicant for business'. These paragraphs apply regardless of any exemptions or thresholds in the Code.

427. AML Code 2008 paragraphs 6, 9, and 11 each set out circumstances under which relevant businesses are able to waive certain requirements for undertaking CDD. However, each of these sections further set out that any such ability or option to waive must be ignored in the event that the business has cause to doubt the identity of the applicant or beneficial owner or it becomes aware of anything that causes it to doubt the bona fides of the applicant or beneficial owner (paragraphs 6(8)(c), 6(8)(d), 9(8)(c), 9(8)(d), 11(11)(c), and 11(11)(d)). The assessors found the IOM compliant with Recommendation 5 in this regard.

Identification measures and verification sources (c. 5.3):

428. AML Code 2008 paragraphs 6(3) and 9(3) provide that financial institutions are required to have in place procedures for: (a) the identification of, and (b) the verification of the identity of the applicant for business using reliable, independent source documents, data, or information. Applicant for business includes any person, natural or legal. The Code also provides for a series of exceptions to the identification requirement which are discussed in detail below in relation to measures applied to low-risk business.

429. For FSC-regulated entities, the FSC Rule Book 2008 Rule 9.6 imposes specific requirements in relation to identification and verification with regard to legal persons and legal arrangements. These provisions are discussed further below.

430. The FSC Handbook Section 4 provides guidance regarding the types of documents and information the FSC considers necessary to fulfill these information and verification requirements. For natural persons, the information has to include name, permanent residential address, date and place of birth, nationality, and gender. Except in the lowest-risk cases or to guard against financial exclusion, information collected should also include an official personal identification number or other unique identifier contained in an unexpired official document. Using a risk-based approach, it may also be warranted to collect information on occupation, name of employer, and source of income and, if applicable, details of any public or high-profile positions held. FSC Handbook Section 4.2.2 sets out the verification procedures in considerable detail and lists the forms of acceptable official and occupation-related documentation. It is evident from the language used in the Handbook that it is in the first instance the responsibility of the licenseholders to satisfy themselves that they have taken

adequate steps to identify and verify the identification of the applicant for business. Considerable discretion is given to the licenseholders in meeting the requirements of the AML Code 2008 and FSC Rule Book. This includes reference to the use of independent electronic data sources to provide confirmatory material, subject to meeting specified quality criteria. There is also guidance to assist in a pragmatic manner where the applicant for business does not possess standard identification information; examples quoted include the elderly, the disabled, students, and minors.

431. For IPA-regulated insurers, IAMLR 2008 Section 9 provides that an insurer must take reasonable measures to verify the identity of the applicant[31] and beneficial owner and satisfy itself as to the source of wealth and funds, using reliable, independent source documents, data or information. Evidence of identity, wherever it appears in the Regulations, shall not be satisfactory unless reasonable measures have been taken by the insurer to identify the applicant. Pursuant to IGN 2.6, all applicants must at a minimum be subject to a standard range of CDD measures including but not limited to the identification of the beneficial owner whilst permitting the application of a risk based approach. The identification and verification requirement applies to natural or legal persons and to legal arrangements.

432. Discretion is permitted in relation to evidence of identity where an insurer can utilize either original or suitably certified copies of identification documentation or 'undertake a form of investigation which has satisfied the insurer as to the identification of the person concerned'. IGN 2.5 restates the verification requirements of the Regulation and expands on the available flexibility of verification procedures in 2.9, covering verification by the insurer non face-to-face; verification by outside agency or using data bases; and verification by use of the internet or other methods.

433. FSC and IPA licenseholders informed the assessors that, in practice, their account-opening or policy application forms include all of the matters set out in the Handbook, the IAMLR 2008, and IGN 2008, as appropriate, together with questions on source of funds and purpose of the business relationship. Verification is usually done by means of an official document (preferably a passport or national identity card, where available), and supported by an original recent utility bill confirming address information. As most of the new applicants for business are nonresident and non face-to-face, often involving the intervention of business introducers, additional risk arises. In practice in such cases, the licenseholders often rely for verification on copy passports, certified by a suitable certifier, as defined. In some cases, the verification is delegated to an eligible introducer, though for insurance business Introducer Certificates are seldom used in practice. In other cases, introducers provide copies of supporting identity/address information. The conduct of this business is also addressed in detail in the assessments of Recommendations 8 and 9.

[31] An 'applicant' is defined as a person or body seeking to effect a contract of insurance with the insurer (whether directly or indirectly) and includes the person(s) beneficially entitled to the assets to be used to fund a premium; any person who is able to exercise control over the policy; and any other person on whose behalf an applicant is acting pursuant to IAMLR 2008 Sections 2 and 10.

Identification of Legal Persons or Other Arrangements (c. 5.4):

5.4(a)

434. With effect from December 18, 2008, a requirement was incorporated under AML Code 2008 paragraph 5(3) that a relevant person must: (a) verify that any person purporting to act on behalf of a legal person or legal arrangement is so authorized, and (b) identify that person and take reasonable steps to verify their identity using reliable and independent source documents, data, or information. For FSC-regulated entities, FSC Rule Book Rule 9.6(3)(a) and (b) also requires that, in the case of a legal person or legal arrangement applicant, the licenseholder must verify that any person purporting to act on behalf of the applicant is authorized to do so and 'identify and verify the identity of that person using reliable and independent source document, data, or information'. Although the requirement did not apply to all relevant financial institutions at the time of the on-site visit, it was introduced shortly afterwards and the assessors were satisfied that the measures were already being applied, in line with prudent business practice, at the time of the assessment.

435. For IPA-regulated insurers in the case of a legal person or body, pursuant to IAMLR 2008 Section 11(1) an insurer is required to confirm the appropriate authorization of any person acting on behalf of the legal person or body and Sections 9(1) by reference to 10(1)(c) requires verification of identity.

5.4(b)

436. AML Code 2008 introduced, effective December 18, 2008, a specific requirement under paragraph 5(3)(e) to verify the legal status of the applicant using relevant information or data obtained from a reliable source. Applicant for business includes any person, natural or legal. [32] Although this requirement did not apply to all relevant financial institutions at the time of the on-site visit, it was introduced shortly afterwards and the assessors were satisfied that the measures were already being applied at the time of the assessment.

437. Moreover, with regard to FSC-regulated entities, FSC Rule Book 2008 Rule 9.6(3) sets out that licenseholders must, inter alia:

- Verify the legal status of an applicant for business using relevant information or data obtained from a reliable source;
- Identify any known beneficiaries in the case of a legal arrangement; and
- Obtain information concerning the names and addresses of the legal person or legal arrangement, any natural person having power to direct its activities, and any person who may (and the means by which they may) impose obligations on the legal person or arrangement.

[32] The Interpretation Act 1976, which applies to every provision of every Act passed after May 1949 defines "person" to cover any person, natural or legal.

438. The FSC Handbook provides additional detailed guidance on the implementation of the provisions for legal persons (Section 4.7) and trusts and other legal arrangements (Section 4.6). With regard to legal persons, the Handbook clarifies that the scope of the term 'legal person' in Rule 9.6 would encompass any body corporate or unincorporated capable of establishing a permanent customer relationship or own property (including e.g., foundations, anstalts, or partnerships). It states that, as Rule 9.6 does not provide any concession for companies administered by corporate service providers, licenseholders are obliged to look through to the directors and signatories of the administered companies. The guidance explains that licenseholders are expected to 'lift the corporate veil' and know the identity of the beneficial owner. It notes that, where the owner is another corporate entity or trust (which is a common occurrence in the IOM), 'reasonable measures' should be taken to verify the identity of the principals.

439. Although not referring to any specific legal provision, the FSC Handbook lists the identification information required for legal persons, including details of registration and of the directors and other persons exercising control, as well as persons authorized to act on behalf of the legal person, including holders of powers of attorney. For 'standard risk' business, at least two of the signatories and two directors should be identified; all must be identified for business deemed to be of higher risk.

440. The FSC Handbook also uses mandatory language in setting out detailed measures to be implemented by licenseholders regarding the identification and verification of trustees and express trusts (to include any other arrangement that has similar legal effect) to supplement FSC Rulebook Rule 9.2(1) and the definition of beneficial owner in the context of a legal arrangement, which includes trustees and settlors. Rule 9.6(3)(c) requires beneficiaries to be identified and Rule 9.8 requires verifying the identity of beneficiaries.

441. For IPA-regulated insurers, in the case of a legal person or body, IAMLR 2008 Section 11 requires an insurer to ascertain the legal status, existence, and identity of the legal person or body, its nature, and the appropriate authorization of any person acting on behalf of the legal person or body; and take reasonable measures to understand the ownership and control structure. Similar to FSC requirements detailed above, the IGN 2008 Sections 4.3–4.15 detail specific requirements relating to evidence of incorporation, details of trustees and directors, memorandum and articles, extracts of trust deeds, and identities of beneficiaries including beneficiaries of trust arrangements.

442. On the basis of the provisions in effect at the time of the on-site visit or shortly thereafter, and of the quality of the implementation observed, the assessors found the IOM to be in compliance with this aspect of Recommendation 5.

Identification of Beneficial Owners (c. 5.5; 5.5.1 & 5.5.2):

443. The requirement to identify beneficial owners is set out in secondary legislation. AML Code 2008 paragraph 2 defines the term 'beneficial owner' using the key sentence of the FATF definition as 'the individual who ultimately owns or controls the applicant for business or on whose behalf a transaction or activity is being conducted'. In relation to a legal person, beneficial owner includes a natural person who:

(a) ultimately owns or controls (directly or indirectly, including through bearer shares) more than 25 percent of the shares or voting rights; or

(b) otherwise exercises control over the management of the legal person.
In the case of a legal arrangement, beneficial owner includes the trustees or other persons controlling the applicant.

444. For FSC-regulated entities, the FSC Rule Book 2008 Rule 9.6.2(a) and (b) also requires licenseholders to determine who is the beneficial owner of the applicant for business. The Rule Book defines the term 'beneficial owner' in Rule 9.2(1) and allows for some pragmatic concessions (broadly consistent with the methodology). The relevant extract from the definition in the Rule Book is as follows:

> 'In relation to a legal person or legal arrangement, [beneficial owner] includes (but is not restricted to):
>
> (a) in the case of a legal person other than a company whose securities are listed on a recognized stock exchange, a natural person who ultimately owns or controls (whether through direct or indirect ownership or control, including through bearer share holdings) more than 25 percent of the shares or voting rights in the legal person; or
>
> (b) in the case of any legal person, a natural person who otherwise exercises control over the management of the legal person;
>
> (c) in the case of a legal arrangement —(i) the trustees or other persons controlling the applicant; and (ii) the settlor or other person by whom the arrangement is made.

445. Rule 9.6 further requires licenseholders to:

- take reasonable steps to verify the identity of the beneficial owner, using relevant information or data obtained from a reliable source; and
- determine whether the applicant is acting on behalf of another person and, if so, to take reasonable steps to identify and verify that other person. (5.5.1)

446. Sections 3 and 4 of the FSC Handbook provide guidance regarding whether a customer is acting on behalf of another person.

447. For IPA regulated insurers, IAMLR 2008 Section 9(1) sets out that the insurer must undertake 'reasonable measures' for identification and verification. However, insurers are also subject to the AML Code 2008 which requires identification in all cases and, in accordance with the FATF Recommendations, provides for 'reasonable measures' for purposes of verification of identity. As noted above, pursuant to IAMLR Section 12, for a beneficiary named or nominated under a life policy, verification can be undertaken at or before the time of a payout of a claim or exercising of rights under the policy. In discussions with insurers, the assessors did not observe any evidence of weaknesses in the implementation of identification procedures.

5.5.1

448. Further to the analysis above, the FSC has provided for a concession from the requirement to identify and verify the beneficial owner. Section 4.12 of the FSC Handbook explains that financial

services businesses (termed 'intermediaries' in relation to this activity) frequently hold funds or assets on behalf of their customers with IOM banks. Examples mentioned in the Handbook include overseas banks (Swiss banks are mentioned as an example in the Handbook) that place deposits on a fiduciary[33] basis with IOM banks. Section 4.12 provides that, where an intermediary acting on behalf of underlying customers falls under the definition of an "Acceptable Applicant"[34], the licenseholder can, subject to specified risk-based conditions, regard the intermediary as its customer and not identify the underlying depositors. The CDD obligations regarding the persons for whom the intermediary is acting rests with the intermediary. The arrangement is analogous to that applied to the funds industry and other pooled investment mechanisms such as unit trusts, to which the provisions of Section 4.12 also apply. In practice, it appears that each distinct holding within the account held in the intermediary's name is identified by a unique reference number. While the concession may be pragmatic, it places significant reputational reliance on the quality of the AML/CFT processes of the originating foreign bank or other 'applicant' and could leave the IOM bank in a difficult position should weaknesses subsequently emerge regarding the quality of the CDD conducted abroad, particularly as—unlike the Eligible Introducer regime described later—there does not appear to be any requirement that the IOM bank identify the ultimate beneficial owner, spot-check the originator's CDD measures, or be in a position to obtain copies of the CDD documentation should it be duly required, for example, for FCU or law enforcement purposes. As the Handbook mentions Swiss banks as an example, the impact of bank secrecy laws there would further ensure that the IOM bank would not be in a position to obtain any information on the beneficial owner of the funds they hold on behalf of customers of their Swiss-bank customers. Due to the underlying risk of misuse, the assessors concluded that this arrangement could not be considered fully compliant, including on a risk-based approach, with Recommendation 5,under which financial institutions should be required to determine whether the customer is acting on behalf of another person and should then take reasonable steps to obtain sufficient identification data to verify the identity of that other person..

5.5.2 (a)

449. With effect from December 18, 2008, and in compliance with Recommendation 5, AML Code 2008 paragraph 5(3)(h) requires financial institutions and other relevant persons to obtain information to understand the ownership and control structure of the applicant.

450. For FSC-regulated entities, Rule 9.6(3)(g) also requires licenseholders to 'take reasonable steps to understand the ownership and control structure of the applicant' where applicants for business are legal persons or legal arrangements. The FSC Handbook provides useful guidance in this respect. For example, the Handbook Section 4.7 indicates that financial institutions should, for corporations and partnerships, "look behind the institution to identify those who have control over the

[33] Fiduciary deposits are a financial product that involve the specific commissioning by a customer of a bank (commonly referred to as the "agent bank") to invest the customer's assets with a third party bank (commonly referred to as the "recipient bank") in the name of the agent bank but for the account and at the sole risk of the customer. The customer normally pays a fee (commission) to the agent bank for the execution of this service.

[34] An Acceptable Applicant is a person regulated by the FCS or IPA, IOM advocate, legal professional, or qualified accountant, or a regulated person from a jurisdiction accepted by the IOM authorities as applying equivalent AML/CFT standards.

business and the company's/partnership's assets, including those who have ultimate control and ultimate principal ownership."

451. For IPA-regulated insurers IAMLR 2008 Section 11(2) requires insurers, in relation to legal persons or bodies, to 'take reasonable measures to understand the ownership and control structure of the legal person or body'. IGN 4.3–4.24 provide considerable supporting detail in relation to publicly listed and private corporate businesses; trustee and nominee structures; various partnership structures; pensions; charities; foundations; and holding companies. The relevant requirements for insurance managers and intermediaries, as they are not within the scope of the IAMLR 2008 and IGN 2008, are contained in AML Code 2008, as discussed above.

452. Based on discussions with financial institutions, the assessors were satisfied that there was already evidence of compliance with this aspect of Recommendation 5 at the time of the on-site visit.

5.5.2 (b)

453. AML Code 2008 paragraph 5(3) introduced a number of requirements relevant to legal arrangements, including requiring relevant persons to identify any known beneficiaries and the settlor (or equivalent). The requirements that apply to applicants for business more broadly are also relevant to legal arrangements and include obtaining information on any natural persons having power to direct activities and information to understand the ownership and control structure. For FSC-regulated entities in relation to legal arrangements, Rule 9.6(3)(c) of the FSC's Rule Book requires licenseholders to identify any known beneficiaries and Rule 9.8 requires licenseholders to have identified a beneficiary and verified their identity before making any payment of capital or income.

454. The FSC Handbook Sections 3 and 4 provide additional guidance as to how these requirements could be met, in particular when the applicant is a legal person: the licenseholder must in that case 'obtain identification information on the underlying principals, i.e., persons exercising control over the management of the legal person, or any person having power to direct the activities of the legal person'. If the customer is a trust, the FSC Handbook explains that the trustee(s) or other persons controlling the applicant must be identified, as well as 'the settlor(s) or any other person by whom the arrangement is made, protector(s), any other person having power to direct the activities of the applicant, any person whose wishes the trustee may be expected to take into account, known beneficiaries, and potential beneficiaries presenting a high risk' (FSC Handbook, Section 3.2.1).

455. For IPA-regulated insurers, in relation to legal arrangements, IAMLR 2008 (9) and (10) require insurers to identify and verify beneficial owners, whether natural or legal, and Section 12 requires insurers to have identified a beneficiary under a life insurance policy and verified their identity before making any payment under a policy.

456. IGN 2008 4.3–4.14 provides considerable detail in relation to the requirements where the applicant is a legal person or body, including a list of officers from whom it can take instructions and their specimen signatures; satisfactory evidence of a corporate investor; verification of identity of controllers holding 25 percent or more and where the controller is another entity lift the veil to the ultimate owner or controller. The insurer must, pursuant to IGN 2008 4.5, where the applicant is a trust, identify the trustee(s) or other persons controlling the applicant including evidence of proper appointment; the settlor(s) or any other person by whom the arrangement is made, protector(s), any

other person having power to direct the activities of the applicant, any person whose wishes the trustee may be expected to take into account, known beneficiaries, and potential beneficiaries, as well as the nature and purpose of the trust and the source or origin of the assets under trust.

457. A further point to take into account in the IOM context is the extent to which financial institutions–mainly the banks–depend on others (eligible introducers or otherwise, from within the IOM or nonresident) to conduct on their behalf the identification and verification procedures. A particular vulnerability may arise in relying on third parties to reliably identify and verify the ultimate beneficial owners. The financial institutions interviewed indicated to the assessors the importance they attach to protecting their reputations by taking care in addressing the beneficial owner challenge, whether or not they rely on third parties and, as such, appeared to be implementing measures equivalent to those subsequently formalized in the AML Code 2008. The issue of reliance on third parties is addressed further in the analysis of Recommendation 9.

Information on Purpose and Nature of Business Relationship (c. 5.6):

458. AML Code 2008 paragraph 6(3)(c) introduced a requirement for financial institutions and other relevant persons to establish, maintain, and operate procedures in relation to new business relationships and to obtain information on the purpose and intended nature of the business relationship.

459. For FSC-regulated entities, relevant and detailed guidance is provided in the discussion in the FSC Handbook Section 3 on CDD measures and the development of client profiles, for which an understanding of the purpose and intended nature of the relationship is essential.

460. For IPA-regulated insurers, IAMLR 2008 Section 14 stipulates that an insurer must satisfy itself (obtaining information where necessary) as to the purpose and intended nature of the business relationship. Moreover, pursuant to IGN 4.5(c), 4.7 (a), and 4.13 (e), this requirement also applies for trustee business; partnerships and unincorporated businesses; and foundations, respectively.

461. Financial institutions interviewed during the assessment confirmed that their account opening or policy application forms, as applicable, included questions in this area, the answers to which would be reviewed carefully as part of their customer acceptance procedures.

Ongoing Due Diligence on Business Relationship (c. 5.7; 5.7.1 & 5.7.2):

462. The requirement to conduct ongoing due diligence is set out in secondary legislation. AML Code 2008 paragraph 15 requires, as did its predecessor, ongoing and effective monitoring of any existing business relationship and scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the institution's knowledge of the customer, their business and risk profile, including, when necessary, the source of funds.

463. For FSC-regulated entities, FSC Rule Book Rule 9.15 requires licenseholders to perform ongoing and effective monitoring whose extent and frequency must be determined on the basis of materiality and risk and in accordance with the licenseholder's current risk assessment. Detailed practical guidance is provided in Sections 3.2.5 and 5 of the FSC Handbook.

464. For IPA-regulated insurers, IAMLR 2008 Section 18(1) replicates this requirement (and in particular for PEPs Section 20(6) reinforces the requirement). IGN 2008 provides detailed requirements in relation to ongoing due diligence in Sections 1.4 (enhanced CDD requirements); 3.4 and 3.5 (PEPs); 5 (existing policyholders and the requirement for ongoing review); and 9.5 (complex and unusual transactions).

465. In discussions with financial institutions, the assessors were largely satisfied that effective ongoing due diligence procedures were in place and being implemented, although there appeared to be significant differences in the scale and scope of the measures across the financial institutions, which could not readily be explained by the application of the risk-based approach.

5.7.2

466. The AML Code 2008 introduced a requirement under paragraph 15(1)(a) to ensure that customer CDD information is reviewed to ensure that it is up to date and appropriate (in particular where the relationship poses a higher risk).

467. Although the assessors were not in a position to review the implementation of this requirement across the full range of financial institutions, in the case of FSC-regulated entities, FSC Rule Book Rule 9.15(1)(a) already required licenseholders to review CDD information held to ensure it is up to date and appropriate 'in particular where the relationship poses a higher risk'. Rule 9.9 further requires enhanced CDD to be undertaken for relationships posing a higher risk.

468. The FSC's Handbook provides guidance on keeping information up to date at Sections 2.1.1, 3.1, 3.2.1, 3.2.5, and 4.7. Section 5 also provides guidance on conducting further CDD procedures where the basis of the relationship changes and undertaking a risk based approach to monitoring including particular considerations for high risk relationships.

469. While IPA-regulated insurers are subject to the relevant requirements set forth in the AML Code 2008, there is no specific parallel requirement in the insurance regulations to maintain up-to-date documents, data, or information, which creates the potential for confusion as to which set of requirements insurers should follow. More broadly, IAMLR 2008 Section 18(1) requires the insurer to continually consider the changing risk profile and circumstances of a policyholder or beneficial owner and consider whether or not additional CDD is required.

470. IGN 2008, while again not specifically requiring or maintaining up-to-date records, includes considerable detail in relation to policies requiring enhanced due diligence and monitoring (1.4); trigger events (5.1); subsequent business transactions not expected by the insurer (5.2); and 5.4 in relation to retrospective risk based reviews of deficient identification documentation per file with a focus on high risk relationships and low-risk relationship reviews on a trigger event basis. The requirements contained therein may be expected to include review of existing records and updating as necessary.

Risk—Enhanced Due Diligence for Higher Risk Customers (c. 5.8):

471. As noted, AML Code 2008 introduced in paragraph 8 a requirement that relevant persons must carry out enhanced CDD where an applicant for business poses a higher risk. Paragraph 8(2)

specifies that higher-risk customers include, but are not restricted to: PEPs; persons in a country that does not apply or insufficiently applies the relevant FATF Recommendations; a person subject to a warning issued by a competent authority; or a company with bearer shares. Other relevant categories of high-risk business listed as examples in the FATF Recommendations (e.g., nonresident customers; private banking; trusts or other personal asset-holding vehicles; and companies with nominee shareholders) are not listed but neither are they excluded from the overall requirement for enhanced diligence for higher-risk business.

472. For FSC-regulated entities, Rule 9.9 of the FSC's Rule Book also deals with circumstances when enhanced CDD must be carried out. These circumstances include (but are not restricted to):

(a) a business relationship with

(i) a politically exposed person; or

(ii) a person or legal arrangement resident or located in a country which the licenseholder has reason to believe does not apply, insufficiently applies , the FATF Recommendations in respect of the business or transaction in question;

(b) a person or legal arrangement which is the subject of a public warning issued by the FSC for the purposes of Rule 9.9

(c) a company which has shares in bearer form.

473. Furthermore, in respect of non face-to-face business, FSC Rule Book Rules 9.6(4) and 9.15(3) require adequate measures to be taken to compensate for any risk arising as a result of the relationship being non face-to-face. Rule 9.11 sets out specific requirements for dealing with relationships with politically exposed persons. These requirements have been included also in AML Code 2008 with regard to all relevant persons at paragraphs 6(6), 7(5), 9(5), and 15(3) with respect to non face-to-face business and at paragraph 10 with respect to politically exposed persons.

474. IPA-regulated insurers must undertake a risk assessment of their clients and those considered to be higher risk must be subject to enhanced due diligence pursuant to IAMLR 2008 Section 13. In addition, IGN 2.6 and 4 provide considerable detail on the risk assessment process to be undertaken at a recommended minimum level, although insurers may adopt a risk-based approach for assessing documentation and require additional or reduced evidence.

475. The IOM authorities recognize that the nature of most of the financial services business in the IOM is potentially high risk, as it is largely nonresident, non face-to-face business and much of it originates through introduced business. The requirements, as extended in late-2008 and supported by detailed guidance in the FSC Handbook and IGN 2008, deal specifically with a range of enhanced due diligence issues to encourage financial institutions, in applying a risk-based approach, to take appropriate account of all categories of customer they regard as high-risk. While the assessors regarded the current approach in the IOM as largely consistent with Recommendation 5, they recommended that the authorities expand the current list of categories of high-risk customers and consider including, for example, private banking and business involving trusts and other legal arrangements.

Risk—Application of Simplified/Reduced CDD Measures when appropriate (c. 5.9):

476. A number of concessions to the standard CDD requirements are provided for in secondary legislation and expanded somewhat in guidance. Having regard to the wording of the relevant FATF Recommendations and published guidance, it is not a straightforward task to determine whether any or all of these concessions are within the scope of FATF Recommendation 5 as representing appropriate reduced or simplified CDD measures, when identifying and verifying the identity of the customer and the beneficial owner where there are low risks. The conclusion for the purposes of this assessment is indicated following the analysis below for each type of concession.

477. AML Code 2008 paragraphs 6(4) and 9(4) provide for what is commonly termed in the IOM the 'Acceptable Applicant' process. This permits both FSC and IPA licenseholders to conduct business with particular types of regulated businesses without having to obtain full CDD documentation for purposes of identity verification. The businesses concerned are listed in the Code as:

a) a regulated person (defined in paragraph 2 of the Code to include specified categories of regulated financial institutions and fiduciaries in the IOM).

b) an advocate within the meaning of the Advocates Act 1976 or legal practitioner within the meaning of the Legal Practitioners Registration Act 1986 or an accountant carrying out business in or from the IOM, where subject to rules of a professional body that include requirements and procedures at least equivalent to the Code;

c) a person who acts in the course of external regulated business (defined in paragraph 2 of the Code to mean a regulated business outside the IOM that corresponds to any of those businesses regulated by the FSC or IPA) and which is regulated under the law and regulations of a country in the list in Schedule 2 to the Code (in which the IOM authorities have listed jurisdictions which, in their view based at least in part on published AML/CFT assessment reports, adequately apply the FATF Recommendations).

478. In order to take advantage of the above concession in accordance with the Code, the licenseholder must:

- know the identity of the applicant for business i.e., it must not be anonymous;
- know the nature and intended purpose of the relationship; and
- be satisfied that the applicant for business is one of the businesses listed at paragraph 6(5) and 9(4) of the Code.

479. Pursuant to paragraphs 6(7) and 9(7) of the Code, the above concession does not apply where the licenseholder has any reason to believe that the country in which the applicant for business is incorporated or formed does not apply or insufficiently applies the FATF Recommendations. Furthermore, under paragraphs 6(8) and 9(8) this concession does not apply where there is knowledge or suspicion of money laundering or terrorist financing or there is doubt about the identity or bona fides of the applicant for business.

480. For IPA-regulated insurers undertaking long-term business, detailed obligations are set out in IGN 2008 Paragraphs 2.13 and 4.1 with respect to business involving Acceptable Applicants, including provision for the Acceptable Applicant to provide verification of identity documents, duly certified. If this documentation is not provided by the Acceptable Applicant, the insurer must itself obtain it. The insurer must monitor the status of the Acceptable Applicant on an ongoing basis.

481. The obligations of insurers notwithstanding, a number of broader issues arise with respect to the scope of the concession:

- It goes beyond the suggested example in the FATF methodology which refers to financial institutions (while this is merely an example, it nonetheless underlines that any concession granted should have a low risk threshold).

- While the inclusion of certain IOM-regulated DNFBPs within the potential scope of the concession (particularly for CSPs and TSPs) may appear justifiable by reference to the AML/CFT measures required of them in the IOM, as noted in section 4 of this report, the AML/CFT measures for a number of relevant categories of DNFBP in the IOM are still in the course of development and implementation. The current scope of AML Code 2008 Paragraphs 6(4)–6(5) and 9(4) could be misinterpreted as already granting the concession without regard to the enhancements still needed in AML/CFT coverage, particularly for advocates and accountants.

- While measures are already in place at least to some degree for IOM advocates, as noted elsewhere in this report there is no basis (and no proposal at the time of the assessment to introduce a basis) for applying or supervising the implementation of AML/CFT measures for non-IOM legal practitioners registered to conduct certain business in the IOM. Yet it would appear that the Acceptable Applicant concession could apply in their case, albeit subject to the external regulated business test.

- The scope of the definition of external regulated business is broad and imposes a challenge (and therefore a heightened risk) for IOM institutions to determine accurately the extent of supervision to which the external regulated businesses are subject and whether or not that supervision adequately addresses AML/CFT matters.

482. In discussions with the assessors, financial institutions confirmed that the Acceptable Applicant facility is used, though they pointed out that they determine on a risk basis the level of due diligence warranted in each case. Having regard to the level of due diligence which many of the institutions opt to conduct in any case, regardless of the available concession, the assessors were not clear of the value of maintaining the Acceptable Applicant concession in its current form. Having regard to the range of issues raised above, the assessors do not consider that the current Acceptable Applicant facility to be fully compatible with the FATF Recommendations, including on a risk-based approach nor with the guidance in the Basel CDD paper.

483. AML Code 2008 paragraph 11 provides a concession in respect of introduced business. This concession is commonly termed the Eligible Introducer's system. This concession allows introducers to maintain the verification documentation relating to the applicant for business being introduced, subject to the controls outlined in the Code. In respect of businesses regulated by the FSC, further

requirements are in place in respect of the Eligible Introducer's system at Rule 9.10 of the FSC's Rule Book. For IPA-regulated insurers, further requirements are specified in respect of an Introducer's Certificate, detailed in IGN 2008 Section 8. The IPA indicated that, insofar as insurance is concerned, Insurance Certificates are seldom used in practice (and by only one insurer) and, even when they are used, they will often be accompanied by supporting identity and address documentation. (The more common practice in the insurance sector is the use of the Acceptable Applicant system, as discussed previously.) The Eligible Introducer concession is addressed in detail in the analysis of Recommendation 9.

484. In respect of businesses regulated by the FSC, the definition of beneficial owner at Rule 9.2 of the FSC's Rule Book allows for a concession where the applicant for business is a company whose securities are listed on a recognized stock exchange. This form of concession is envisaged in the FATF methodology.

485. The FSC's AML/CFT Handbook set out certain concessions which do not appear to have a clear legal basis in either the AML Code 2007 or 2008 or FSC Rule Book. FSC Handbook Section 4.8 offers a pragmatic clarification in relation to employee benefit schemes, share option plans, and pension schemes that it is the trustee, controller, administrator, or scheme manager who is the principal to be identified and verified for CDD purposes. This concession is broadly consistent with the FATF Recommendations, but, although it purports to grant an exemption from a requirement in secondary legislation, it does not appear to have been provided for in the IOM in law, but only in guidance.

486. FSC Handbook Section 4.10 describes a further concession that can apply (but for which no legal basis is indicated) 'where the ML and FT risk has been assessed to be at its lowest' (e.g., savings accounts) to permit licenseholders to accept source of funds as evidence of identity. Certain conditions must be met to limit the risk of this concession, as follows. Where:

a) All initial and future payments are made from a financial services product or account in the name of the customer that is held with another local regulated financial services business or regulated financial services business in an equivalent jurisdiction; and

b) No initial or future payments may be made by or received from third parties; and

c) The funds can only be repaid to the customer; and

d) Cash payments are not permitted with the exception of face-to-face withdrawals by the customer where evidence of identity is required to be produced before the withdrawal can be made; and

e) There is no suspicion of money laundering or terrorist financing,

a licenseholder may take the view that satisfactory verification has been achieved without the need for additional evidence of identity or address. However, the concession will be in respect of this product or service only.

487. While the assessors accept that the above conditions, where met, should significantly limit ML or FT risk arising from this activity, they do not entirely eliminate the scope for abuse. For

example, the requirement that funds may be repaid only to the customer does not specify that such repayment may only be in the same form, currency, and to the same account or location as the source of funds. It is not clear, therefore, that this facility is entirely compatible with the FATF Recommendations (which provide for simplified or reduced measures when identifying or verifying identity—rather than no verification measures—where the risk is lower, or with applicable primary and secondary legislation in the IOM, which does not appear to explicitly provide the power to grant such an exception. The assessors understand that the use of this facility is not material in the IOM.

488. As noted earlier, Section 4.12 of the FSC Handbook provides that financial services businesses (termed 'intermediaries' in relation to this activity) frequently hold funds or assets on behalf of their customers with IOM banks. Examples include overseas banks (the Handbook refers to Swiss banks) that place deposits on a fiduciary basis with IOM banks. Section 4.12 provides that, where an intermediary acting on behalf of underlying customers falls under the definition of an 'Acceptable Applicant', the licenseholder can, subject to specified risk-based conditions, regard the intermediary as its customer and not identify the underlying depositors. The CDD obligations regarding the persons for whom the intermediary is acting rests with the intermediary. The arrangement is analogous to that typically applied to the funds industry and other pooled investment mechanisms such as unit trusts, to which the provisions of Section 4.12 also apply. However, the assessors could not identify any legal basis in either the AML Code 2007, AML Code 2008, or FSC Rule Book to support this concession. As noted above, the assessors concluded that this arrangement is not compliant with Recommendation 5, under which financial institutions should be required to determine whether a customer is acting on behalf of another person and should take reasonable steps to obtain sufficient identification data to verify the identity of that other person.

489. For IPA regulated insurers, a number of concessions for reduced or delayed CDD are permitted pursuant to IAMLR 2008 Section 7(1) These concessions relate to monetary thresholds of a single premium and accumulated related premium in a calendar year, as detailed above. Section 7 (2) permits concessions where the policy in question has no surrender or maturity value. Where concessions apply pursuant to Section 7, CDD must still be undertaken before a payout under the contract.

490. The requirements for publicly listed companies on a recognized stock exchange are less detailed than other corporate business structures in IGN 4.3 reflecting the differing levels of risk arising. IGN 2.6 details the recommended starting measures of CDD and 1.2 states that where deviation from the Guidance Notes occurs, it can only be done so on a justified case-by-case basis and approved by senior management or by genre of business and approved by the Board of Directors of the insurer. Pursuant to Section 1.3, any deviation from or variation to the standard requirements set out in the Guidance Notes may be considered on its own merits by the courts.

491. IAMLR 2008 Section 13(3) does not permit the use of the concessions if the application is considered a higher risk or there is a suspicion of ML/FT.

Risk—Simplification / Reduction of CDD Measures relating to overseas residents (c. 5.10):

492. The concessions discussed above, and those arising under the Eligible Introducer arrangements, are restricted to countries listed in Schedule 2 of the AML Code 2008. This list was prepared by the DHA in consultation with the FSC and IPA as a list of selected FATF members and

other jurisdictions that the IOM authorities are satisfied adequately meet the FATF Recommendations. However, whether or not the jurisdiction is listed in Schedule 2 of the Code, if the licenseholder or other relevant person has any reason to believe that the jurisdiction in question does not apply, or insufficiently applies, the FATF Recommendations in respect of the business of that person, the concessions cannot be applied. This prohibition is set out in AML Code 2008 paragraphs 6(7), 9(7), and 11(6) in respect of introduced business and complies with Recommendation 5.

Risk—Simplified/Reduced CDD Measures Not to Apply when Suspicions of ML/TF or other high risk scenarios exist (c. 5.11):

493. In line with Recommendation 5, the listed concessions are not allowed by AML Code 2008 paragraphs 6(8) , 9(8), and 11(11) where there is any knowledge or suspicion of ML. As noted, the Code defines money laundering to also include FT, the legal basis for which was discussed earlier. However, the Code makes no reference to disapplying the concessions where specific high-risk scenarios apply.

494. In respect of FSC-regulated entities, as there is no clear legal basis under the Code for the concessions described above arising under FSC Handbook sections 4.8, 4.10, and 4.12, it is also unclear whether they would be subject to the disallowance in the Code relating to any knowledge or suspicion of ML. Moreover, there is no direct prohibition in the FSC's Rule Book from conducting the simplified CDD measures of paragraphs 6(4), 9(4), and 11 where specific higher risk scenarios apply. However, Rule 9.5 of the Rule Book requires FSC licenseholders to apply CDD measures on the basis of materiality and risk. Rule 9.9 requires enhanced CDD to be undertaken in respect of certain higher risk relationships and Rule 9.11 applies further requirements in respect of relationships involving politically exposed persons. Furthermore, Rule 9.15 requires appropriate ongoing monitoring of all relationships. Where simplified CDD had been applied at the outset of the relationship, and through the ongoing monitoring requirement it was found that higher risk scenarios applied, the requirements at 9.15(1)(a) would come into effect and the FSC licenseholder would need to take steps to ensure the CDD obtained was appropriate. There are also parallel requirements in the AML Code 2008 to those quoted from the FSC Rule Book in the second half of this paragraph.

495. For IPA-regulated insurers, as discussed above, IAMLR 2008 Section 13(3) does not permit the use of the concessions, including reduced or simplified CDD, if the application is considered a higher risk or there is a suspicion of ML or FT.

Risk Based Application of CDD to be Consistent with Guidelines (c. 5.12):

496. In respect of the concessions provided by the AML Code 2008 as outlined above, the Code does not contain any provisions that the implementation of CDD measures on a risk-sensitive basis should be conducted in consistence with guidelines issued by competent authorities. However, paragraph 4(3)(a) of the Code states that where a Court is determining whether a person has complied with any of the requirements of the Code, the Court may take account of any regulatory guidance applied to that person by a competent authority, which is defined in paragraph 2 to include the FSC and the IPA. Moreover, AML Code 2008 introduced with effect from December 18, 2008, a requirement that relevant persons must conduct risk assessments which, the assessors accept, would be expected to take into account relevant guidance issued by the authorities.

497. For FSC-regulated entities, extensive guidance is provided in the FSC Handbook, including in relation to the implementation of the specified concessions.

498. The IPA requires a risk sensitive approach pursuant to IAMLR 2008 Section 13 and sets out the basis under which risk assessment and the application of an appropriate standard of CDD must be performed by the insurer. Extensive details on a minimum recommended standard and implementation and treatment of concessions is contained in the Guidance Notes.

Timing of Verification of Identity—General Rule (c. 5.13): Timing of Verification of Identity—Treatment of Exceptional Circumstances (c.5.14 & 5.14.1):

499. With regard to the timing of CDD measures, AML Code 2008 paragraph 6(2) addresses new business relationships and requires that identification and verification of identity must take place before a business relationship is entered into, or during the formation of that relationship, but in any event it must take place as soon as reasonably practicable (taking into account the need not to interrupt the normal conduct of business where there is little risk of money laundering or terrorist financing occurring) after contact is first made between the relevant person and the applicant for business. AML Code 2008 paragraph 9(2) applies relevant requirements in relation to one-off transactions and Paragraph 11(3) in relation to introduced business. However, unlike the provisions for new business relationships, these paragraphs require identification and verification to be completed before entering into a transaction or a relationship, respectively.

500. For FSC-regulated entities, FSC Rule Book Rule 9.6(5) stipulates that licenseholders must not proceed with a business relationship or transaction unless they have determined who is the beneficial owner and taken reasonable steps to verify that beneficial owner and, where appropriate, applied specified basic CDD measures to customers that are legal persons or arrangements, with enhanced measures for non face-to-face business. In the case of a legal arrangement, Rule 9.8 of the FSC's Rule Book permits licenseholders to verify the identity of beneficiaries after a relationship has commenced but it must be completed before any payment of income or capital is made.

501. There appear to be differences in the scope of the timing requirements of the AML Code 2008 and the FSC Rule Book which could create the potential for confusion and conflict. However, the FSC's Handbook Section 4.13 provides some guidance to clarify that licenseholders must complete identification and verification procedures before entering into a business relationship. However, in exceptional circumstances, where there is little risk of money laundering or terrorist financing, identification and verification procedures may be carried out as soon as reasonably practicable if it is essential not to interrupt the normal conduct of business. This is subject to certain controls that are outlined at Section 4.13 of the Handbook and apply in cases where identification and verification has not been completed at the outset, requiring senior management approval and monitoring, management of ML and FT risks, limiting of types and amounts of transactions, and monitoring of large, complex, or unexpected transactions. While this is useful, it does not resolve the basic differences in terminology between the AML Code 2008 and the FSC Rule Book.

502. For IPA-regulated insurers, IAMLR 2008 Section 9(1) requires that insurers must not proceed with a business relationship unless they have conducted CDD. Timing of CDD concessions regarding the beneficiary of a life policy is permissible pursuant to Section 12 whereby verification of the identity of beneficiaries can be obtained after a relationship has commenced but must be completed

before any payment is made under the contract. This concession is not available if the beneficiary of a life policy is also an applicant under the same policy.

503. The FATF standard allows some discretion to defer the completion of initial CDD and among the examples quoted by the FATF methodology is non face-to-face business, which is the norm in the IOM. In discussions with financial institutions, the assessors were informed that it is common in the IOM for new business to be accepted prior to the completion of CDD measures. Some institutions would allow up to 30 days for all verification documentation to be submitted; at least one institution would allow up to 60 days. In most—but not all—cases, active business would not be allowed to commence on the account prior to completion of all relevant CDD measures. Most institutions indicated that delays typically related only to a minor technical deficiency such as a poorly-photocopied or outdated verification document, rather than a complete absence of initial due diligence. The decision to accept the customer and to allow the business to commence would be taken on a case-by-case basis in accordance with internal procedures and taking into account potential ML or FT risk. Nonetheless, it appeared to the assessors that financial institutions were prepared to offer unusual levels of flexibility regarding the conducting of financial business in advance of completing full CDD which could potentially impact on the effectiveness of the AML/CFT measures. A further example was identified in discussions with legal and accounting professionals—some of whom introduce business to financial institutions—that, in allowing themselves up to three months to complete the CDD, situations arise where the business with their client is completed within that timeframe, the client relationship does not have reason to continue, and, in reality, CDD is never conducted. This is a concern from the perspective of any financial institution relying on the professional to have completed the CDD.

504. Overall, therefore, while the IOM requirements are broadly consistent with Recommendation 5, some questions remain regarding the effectiveness of some aspects of implementation and particular attention by the regulatory authorities to the issue of delayed CDD may be warranted in future onsite inspection work.

Failure to Complete CDD before commencing the Business Relationship (c. 5.15):

505. In line with Recommendation 5, paragraph 4(2) of the AML Code 2008 makes it an offense for any person who contravenes the requirement not to form a business relationship or carry out a one-off transaction with or for another person nor continue a business relationship unless that relevant person establishes, maintains, and operates CDD procedures (referred to as identification procedures in the Code) as set out in AML Code 2008 paragraphs 5 to 15 (i.e., new business, existing business, and one-off and introduced business relationships). Pursuant to AML Code 2008 paragraph 6(9), 7(6), 9(9), and 11(12), in any case where a relevant person, including a financial institution, does not succeed in completing the identification and verification as required under the Code, the business relationship and transactions shall not proceed any further, the relationship shall be terminated, and the relevant person shall consider whether to file an STR.

506. For FSC-regulated entities, the prohibition on proceeding with a business relationship or transaction is repeated in FSC Rule Book Rule 9.6(5). The FSC's Handbook provides further guidance at Section 4.13.1. The FSC Handbook also sets out, in Section 4.13.1, that where verification of identity cannot be concluded within a reasonable timeframe and without adequate explanation, licenseholders must assess whether the circumstances are in themselves suspicious. In

such circumstances licenseholders must consider making a disclosure/suspicious transaction report to the FCU. FSC Handbook Section 5.4.4 also provides guidance on the types of situations giving rise to suspicion which includes 'where the customer refuses to provide the information requested without reasonable explanation'. FSC Handbook Section 6.5 also provides guidance on reporting declined business to the FCU where there is knowledge or suspicion of money laundering or terrorist financing.

507. IPA-regulated insurers are required, pursuant to IAMLR 2008 Section 16, to consider making a suspicious transaction report to the FCU when the insurer is unable to obtain satisfactory evidence of identity and throughout the policy's lifetime, including for any claim payment (Section18(2)). Additionally, IGN Section 9.4(a) provides examples of insufficient identity verification as triggers for suspicion which may necessitate the making of a suspicious transaction report.

508. In practice, financial institutions interviewed in the course of the assessment confirmed that they would and do refer suspicions to the FCU in cases where they have difficulty in obtaining full CDD information from existing and prospective customers, and that they file STRs where warranted. This information was confirmed by the FCU.

Failure to Complete CDD after commencing the Business Relationship (c. 5.16):

509. In the context of continuing business relationships under AML Code 2008, paragraph 7(6) requires that the business relationship shall not proceed any further in the event that satisfactory CDD information and verification documentation (referred to in the Code as evidence of identity) is not obtained or produced, the relevant person shall consider terminating the relationship, and consider whether to file an STR.

510. For FSC-regulated entities, FSC Rule Book Rule 9.6(5) requires that licenseholders 'must not proceed with the business relationship or transaction in question' unless the CDD requirements contained at Rule 9.6 have been complied with. Section 6.5 of the FSC's AML/CFT Handbook also provides guidance on reporting declined business to the FCU where there is knowledge or suspicion of ML or FT.

511. Similar to the FSC requirements, IAMLR Section 9(1) requires that, in the absence of satisfactory evidence to verify the identity, the application for a business relationship must not proceed any further. This requirement is continued throughout the IGN 2008.

Existing Customers—CDD Requirements (c. 5.17):

512. AML Code 2008 Paragraph 7(2) requires a relevant person, including a financial institution, to apply CDD requirements to existing business relationships, including upon the occurrence of defined 'triggers' relating to perceived changes in circumstances. This includes where anything arises to cause doubt as to the adequacy of CDD information and documentation already held. IGN 2008 Paragraph 5 sets forth the obligations of IPA-regulated long-term insurers in relation to the ongoing review of existing policyholders. The requirements are detailed and include trigger events such as subsequent business transactions or any redemption request. The FSC pointed out that there are relevant obligations for FSC-regulated entities under Rule 9.4 of the FSC Rule Book such that, in conducting the mandated risk assessment, licenseholders must cover existing relationships, including

a review of information and documentation held.[35] While the position as regards implementation was not totally clarified in discussions with financial institutions, the assessors understand that a program of reidentification was undertaken, on the basis of materiality and risk, when the standard for CDD requirements was increased substantially in 2003/4 and that the work on the above-mentioned risk assessments had commenced.

Existing Anonymous-account Customers – CDD Requirements (c. 5.18):

513. No cases of anonymous accounts were identified to the assessors. Should such a case ever arise, AML Code 2008 paragraph 7 requires that, where a financial institution or other relevant person becomes aware that the CDD information or documentation held is inadequate, they must take steps to obtain adequate information or documentation.

Analysis of Effectiveness – R.5

514. The measures outlined above were in force and effect at the time of the assessment and are, therefore, properly taken into account for purposes of this report. It is difficult, however, to provide in all cases an accurate assessment on the effectiveness of their implementation as a number of them were introduced only shortly before the on-site visit or brought into force and effect within a short time thereafter, as follows:

	Effective date:
AML Code 2007[36]	September 1, 2007
AML Code 2008	December 18, 2008
FSC Rule Book	August 1, 2008
FSC Handbook	August 1, 2008
Insurance Act 2008	December 1, 2008
IPA Insurance (Anti-Money Laundering) Regulations 2008 (IAMLR 2008)	September 1, 2008
IPA Guidance Notes on Anti-Money Laundering and Preventing of the Financing of Terrorism – for Insurers (Long Term Business) (IGN 2008)	September 1, 2008

[35] The issue of grandfathering is addressed more explicitly in the post-assessment version of the FSC's Handbook issued in January 2009.

[36] Superseded by the AML Code 2008

515. The authorities and the financial institutions indicated that the revised Code and the most recent materials have been through a number of consultation phases which has allowed the financial institutions to internalize their provisions even prior to their coming into effect. Moreover, many of the changes represented an upgrading of the legal status of preexisting guidance by incorporation into regulations. However, the regulatory authorities have, in the main, not yet had the opportunity to assess the implementation of the recent changes by means of on-site visits. The FSC and the IPA had plans to do so from early 2009, although the FSC pointed out that they had included the guidance in question within the scope of their inspection work in recent years. While taking into account all evidence obtained from financial institutions during the course of the onsite visit, however, the assessors are constrained in assessing the effectiveness of implementation of some of the provisions, in particular, those introduced through AML Code 2008.

516. In meetings with financial institutions (as well as, in some cases their auditors and legal advisors), the assessors found a very high level of awareness of AML/CFT risks and requirements. It was evident that many of the institutions had been closely involved in supporting the development of the latest CDD measures and understood well the rationale for them. Many noted the degree of change in attitude to AML/CFT compliance issues, both within the institutions and among their client base, since the last assessment in 2002/3. The majority of financial institutions are part of UK, Irish, or other international financial services groups and are required to comply with group AML/CFT policies and procedures as well as the requirements in the IOM. Many, as part of international financial groups, already have experience in implementing a risk-based approach to ML/FT detection and prevention. Overall, the responses received by the assessors pointed to a high level of compliance with the CDD requirements, though it was not possible for the assessors to test this directly.

517. Almost all institutions interviewed stressed that they apply the CDD measures using the permitted risk-based approach. While such an approach has merit, it also has the effect of making internal management and regulation more difficult as it increases the scope for subjective judgment on the part of the institutions. If not carefully managed and documented, the risk-based approach could be a source of increased ML and FT vulnerability. It appeared to the assessors that, in some cases, the risk-based approach was being offered as an explanation for less than full compliance with some aspects of the IOM requirements and it is recommended that the regulatory authorities include testing in this regard as part of the on-site visit program.

518. Closely linked to a discussion of the impact of the risk-based approach is the high-risk profile of much of the financial sector business in the IOM (nonresident, non face-to-face, and often introduced by third parties, or involving the management of financial institutions from the IOM, with concessionary arrangements for identification, certification, and verification of the customer and the beneficial owner, if different). The assessors recognize that much of the business, though matching this profile, is in reality not high risk and is easily understood by the financial institutions. However, the degree of reliance on others, particularly outside the supervisory reach of the IOM authorities, clearly gives rise to increased risk and it was not evident to the assessors that all of the financial institutions took this fully into account in applying their AML/CFT procedures. While some institutions indicated a tightly controlled and cautious approach to the limited use of such arrangements as the Suitable Certifier, Eligible Introducer, or Acceptable Applicant, others were open to using any or all of these facilities, in combination, without indicating any particular need for enhanced due diligence. It could be expected, therefore, that the quality of implementation of the required AML/CFT CDD measures might be uneven, and heavily dependent on the quality of the due

diligence work conducted by Eligible Introducers and others to whom the work (although not the ultimate responsibility) is delegated, operating either in the IOM or abroad.

Foreign PEPs—Requirement to Identify (c. 6.1):

519. With effect from December 18, 2008, AML Code 2008 paragraph 10 introduced requirements in line with Recommendation 6 for relevant persons to maintain appropriate procedures and controls to determine whether an applicant for business, a customer, or a beneficial owner or controller is a politically exposed person (PEP). The term PEP is defined in detail in AML Code 2008 Paragraph 2 to include an extensive range of nonresident officials and those holding other relevant positions, together with their close relatives and associates.

520. For FSC-regulated entities, FSC Rule Book Rule 9.2 also provides a detailed definition of a PEP covering all aspects of the definition in the FATF glossary. It includes a list of categories of natural persons entrusted with prominent public functions, a list of categories of their family members, and a list of categories of close associates. Domestic PEPs are excluded from the FSC definition.

521. FSC Rule Book Rule 9.11 requires licenseholders to maintain appropriate procedures and controls to determine whether an applicant for business, an existing customer, or beneficial owner or controller is a PEP. Guidance in relation to PEPs in included in the FSC Handbook Section 3.5.

522. For IPA-regulated insurers, IAMLR 2008 Section 2 defines PEPs as natural persons entrusted with prominent public functions, their immediate family members, or persons known to have influence over the decisions of such persons. The IGN 2008 extends the PEP definition to include close associates and a list of natural persons entrusted with prominent public functions, a list of categories of their family members, a list of categories of close associates, and a list of legal PEPs. The definition contained in IGN 2008 is in line with the FATF glossary whereas that in IAMLR 2008 does not expressly include persons who have previously held such a position. While this inconsistency does not impact on the assessment, as the binding guidance notes have been accepted as other enforceable means and, therefore, provide a sufficient legal basis for PEP-related requirements, it would be preferable to also bring the definition in IAMLR 2008 into line with the international standard. In this case, domestic PEPs are not excluded from the definition, although they are outside the scope of the definition of the AML Code 2008.

523. Pursuant to IAMLR 2008 Section 20, regulated entities are required to maintain procedures to determine whether the applicant, policyholder, beneficial owner, person funding the premium, a settler or trustee, named or nominated beneficiary, or a natural person having power to direct the activities of the applicant or policyholder is a PEP. In such instances, simplified or reduced CDD must not be applied.

Foreign PEPs—Risk Management (c. 6.2; 6.2.1):

524. AML Code 2008 Paragraph 10(2) requires relevant persons to maintain procedures for obtaining senior management approval to establish a business relationship or conduct a one-off transaction with a PEP, or to continue a business relationship with a customer who is discovered to be a PEP.

525. For FSC-regulated entities, FSC Rule Book Rule 9.11(2) also requires licenseholders to maintain appropriate procedures and controls for requiring the approval of its senior management, before establishing a business relationship or continuing an existing business relationship with a PEP. The FSC Handbook Section 3.5 reiterates the requirement for senior management approval and calls for a regular review, on at least an annual basis, of the development of the relationship.

526. FSC Rulebook Rule 9.11(2)(b) stipulates that when a PEP is identified as being involved in existing business the approval of the licenseholder's senior management is required to continue that business relationship. This is reiterated in Section 3.5 of the FSC Handbook.

527. On the identification of a prospective client as a PEP, IAMLR 2008 Section 20(4) requires IPA-regulated insurers to apply procedures and controls for senior management approval to accept an application for a business relationship. Guidance Notes IGN 2008 Section 3.3 further requires senior management involvement and approval, documentation of such approval, and retention of the documentation.

Foreign PEPs—Requirement to Determine Source of Wealth and Funds (c. 6.3):

528. AML Code 2008 paragraph 6(3)(d) introduced a requirement applicable to all new business relationships, which would include PEPs, that relevant persons take reasonable steps to establish the source of funds of an applicant for business. Moreover, FSC Rule Book Rule 9.7 requires licenseholders to take all reasonable steps to establish the source of funds for all customers, which would include any PEPs. FSC Rule Book Rule 9.9, in applying a requirement to apply enhanced due diligence measures to PEPs Rule 9.9 stipulates that licenseholders must take reasonable measures to establish the source of the wealth of the customer and of any beneficial owner when a PEP is involved in a business relationship.

529. For IPA-regulated insurers, the requirement to establish source of funds and source of wealth pursuant to IAMLR Section 9.1 and 24 is also a general business requirement and not an explicit requirement for PEPs. The IGN 2008 require that where a PEP is identified, higher due diligence requirements should apply, including making additional enquiries into the source of wealth pursuant to Section 1.4.

Foreign PEPs—Ongoing Monitoring (c. 6.4):

530. With application to all relevant persons, AML Code 2008 paragraph 8(3) includes as one of the enhanced due diligence measures a requirement to take reasonable steps to establish the source of the wealth of the customer and any beneficial owner for business categories that may pose a higher risk which are defined in paragraph 8(2) to include PEPs. For FSC-regulated entities, FSC Rule Book Rules 9.9 and 9.15 require enhanced ongoing monitoring of a business relationship involving a PEP. Further guidance in this regard is set out in the FSC Handbook Section 5.1.1.

531. Insurers regulated by the IPA are required to undertake ongoing oversight of policies which have a PEP as a policyholder, beneficial owner, settler, trustee, or beneficiary, pursuant to IAMLR 2008 Section 20(6) and IGN 2008 3.4.

Domestic PEPs—Requirements (Additional Element c. 6.5):

532. The IOM requirements do not extend to domestic PEPs for FSC licenseholders. However, the assessors found that, in practice, a number of banks appear to be applying the measures also to domestic PEPs.

533. In relation to the IPA regulated insurers, the IAMLR 2008 and the IGN 2008 do not exclude domestic IOM PEPS.

Domestic PEPs—Ratification of the Merida Convention (Additional Element c. 6.6):

534. As the IOM is not a Sovereign State it cannot sign or ratify the UN Convention against Corruption in its own right. The UK is responsible for the IOM's international relations and representing the IOM at multilateral treaty bodies and following consultation with, and the approval of, the IOM Government it may arrange for ratification of conventions to be extended to include the IOM. The UK Government will only agree to extend its ratification of a convention to the IOM once it is content that the IOM's legislation, policy, and practice adequately implements the convention's provisions. In the area of anti-corruption, the IOM has enacted a revised Corruption Act in July 2008. The Council of Ministers agreed in May 2007 that the UK's ratification of the Merida Convention should be extended to include the IOM and that IOM legislation should be amended to allow this to take place. The new Corruption Act was the most significant part of this process, which was designed to bring the IOM provisions largely into compliance with the Convention, but a number of ancillary legislative provisions are being progressed by the authorities to extend the UK's ratification to the IOM.

Effectiveness of implementation – R.6

535. Financial institutions interviewed during the assessment all identified PEPs as being among their higher-risk categories of customer which attracted enhanced due diligence in accordance with their internal control procedures. None indicated any particular difficulty in implementing that due diligence in practice. All appeared to have access to well-known international database products to allow them to determine whether new or existing customers might qualify as PEPs—in some cases, the check was automated and integrated into account and transaction-processing systems; in other cases the checking was done manually. A number of banks indicated that they opted to include domestic IOM PEPs within the scope of their enhanced due diligence.

Cross Border Correspondent Accounts and Similar Relationships (c. 7.1–7.4)

536. With effect from December 18, 2008, AML Code 2008 paragraph 13 introduced a set of requirements in relation to correspondent banking in line with the FATF Recommendations. Using the same language, FSC Rule Book. Rule 9.12 also sets out requirements for FSC licenseholders should they provide correspondent banking services. Rule 9.12 applies to a business relationship or one-off transaction, as the case may be, which involves correspondent banking services or similar arrangements.

537. Pursuant to AML Code 2008 paragraph 13(4) and FSC Rule 9.12, before entering into a relationship or transaction, a licenseholder must:

(a) obtain sufficient information about the respondent bank to understand fully the nature of its business;

(b) determine from publicly available information:

(i) the reputation of the respondent bank,

(ii) the quality of the supervision to which it is subject, and

(iii) whether it has been subject to investigation or regulatory action with respect to money laundering or the financing of terrorism;

(c) assess the procedures and controls maintained by the respondent bank for preventing money laundering or the financing of terrorism, and ascertain that they are adequate and effective;

(d) ensure that the approval of the licenseholder's senior management is obtained; and

(e) document the respective responsibilities of the licenseholder and the respondent bank with respect to measures to prevent money laundering and the financing of terrorism.

Payable-Through Accounts (c. 7.5):

538. Pursuant to AML Code 2008 paragraph 13(5) and FSC Rule Book Rule 9.12(5), where a relationship or transaction involves a payable-through account, a licenseholder must be satisfied that the respondent bank:

(a) has taken steps complying with the requirements of Recommendation 5 (customer due diligence and record keeping) with respect to every customer having direct access to the account; and

(b) will provide the licenseholder on request with relevant evidence of the identity of the customer.

Effectiveness of implementation – R. 7

539. IOM banks are not in the business of providing correspondent banking services on a cross-border basis. Some IOM subsidiaries of UK clearing banks provide clearing services to smaller banks in the IOM, but no case was identified to the assessors that would constitute cross-border correspondent banking or the use of payable-through accounts.

Misuse of New Technology for ML/FT (c. 8.1):

540. AML Code 2008 paragraph 23 introduced a requirement that relevant persons maintain appropriate procedures and controls to prevent the misuse of technological developments, in line with one of the key provisions of Recommendation 8. For FSC-regulated entities effective August 1, 2008, using the same language, FSC Rule Book Rule 9.13 also requires that licenseholders maintain appropriate procedures and controls to prevent the misuse of technological developments for ML or

FT purposes. This is supported by limited guidance in the FSC Handbook Section 2.8 which advises licenseholders to ensure that staff are kept abreast of relevant technological developments and identified methodologies in ML and FT schemes. FSC licenseholders are further advised in the Handbook that the risks and impact that any technological developments may have on their products or services should be fed back into the business risk assessment required at FSC Rule Book Rule 9.4.

541. However, neither the requirements nor the guidance refer to any particular types of technological risks such as internet banking (establishing new account relationships by internet or providing services on a non face-to-face basis electronically to existing customers); the use of credit/debit cards as part of account relationships, particularly to nonresidents on a non face-to-face basis; security of computer systems, particularly if customer-accessible, to address the risk of fraud, phishing, or other improper access to customer information. While it is not necessary to address such matters in primary or secondary legislation, it would be helpful, perhaps in conjunction with the financial institutions, to develop more detailed guidance to improve the effectiveness of the current basic requirements, rather then merely paraphrasing the wording of the FATF recommendation, particularly having regard to the importance in the IOM of non face-to-face relationships. The authorities pointed out in response that they have provided relevant training on a number of aspects of IT abuse and have followed the FATF methodology.

542. A number of financial institutions confirmed to the assessors that, while prospective customers can access account-opening forms on the internet, it is not possible to open an account without forwarding hard-copy documentation, with an original signature. Reference was made, however, to the emergence of certain UK-based financial services products that are being marketed, including in the IOM, on the basis that the customer relationship can be created using the internet. Financial institutions confirmed to the assessors that their services included the issue of debit and credit cards to nonresidents as a means of giving them access to their funds in the IOM. While this is normal banking business, when combined with the likelihood that the accounts were opened on a non face-to-face basis, while relying on a third party to conduct the CDD, the scenario may merit the issuing of additional guidance by the authorities.

543. For IPA-regulated insurers, IAMLR 2008 Section 37 requires insurers to have procedures in place to regularly consider, and have policies in place and take such measures that are needed to prevent the misuse of technological developments for ML or FT purposes. The training requirement pursuant to Section 32 extends to training for all staff on information on new developments, techniques and trends. IGN Section 2.23 refers directly to IAMLR 2008 Section 37 and expands on the topic of misuse of technological development for ML/FT purposes. The reviews of technological developments can be undertaken on a risk-assessed basis and such reviews are considered particularly relevant where application or other contact is made by electronic methods.

Risk of Non-Face to Face Business Relationships (c. 8.2 & 8.2.1):

544. With effect from December 18, 2008, the AML Code 2008 added a requirement into each of the relevant CDD measures that relevant persons take adequate measures to compensate for any risk arising as a result of dealing with an applicant for business otherwise than face-to-face (paragraphs 5(5), 6(6), 7(5), 9(5), and 15(3). In addition, from August 1, 2008, for FSC-regulated entities, pursuant to FSC Rule Book Rule 9.15(3), licenseholders must take adequate measures to compensate

for any risk as a result of not dealing face-to-face with the customer. None of the requirements specify the types of measures that should be applied to non face-to-face business.

545. The FSC Handbook Section 4.5 includes additional guidance, though worded in mandatory terms although the Handbook is not directly enforceable. Section 4.5 provides that, to guard against this increased risk of identity fraud when a customer relationship is established remotely a licenseholder must either:

(a) Obtain copies of documents that have been certified by a suitable certifier; or

(b) If suitably certified copy documents cannot be obtained, address can be verified using electronic data sources, and at least one of the following checks must be undertaken and recorded prior to full activation of the relationship:

(a) Require payment for the product or service to be drawn from an account in the customer's name at a credit institution in an equivalent jurisdiction.

(b) Send a letter by registered post to validate the address of the customer and ensure that the account is not activated until the signed acknowledgement of receipt is returned.

(c) Make a "physical" validation, e.g. an initial telephone call by a member of staff of the financial services business to a telephone number that has been independently validated.

(d) Requisition additional documents to complement those required for face-to-face customers.

(e) Internet sign-on following verification procedures where the customer uses security codes, tokens and/or other passwords which have been provided by mail (or secure delivery) to the named person at an independently verified address.

546. While the above guidance is helpful, it is also indicative of the additional risks arising from non face-to-face business, particularly when use is made of modern technology. As the guidance purports to be mandatory, it would be more appropriate to elevate it (or at least the essential elements) to an instrument that has direct legal effect, such as the FSC Rule Book. There is also scope to add more detailed guidance in the Handbook to emphasize further the risks inherent in non face-to-face business and the recommended additional steps that licenseholders should take to mitigate that risk.

547. IAMLR 2008 Section 13 requires an insurer to assess each applicant or policyholder on a risk basis in order to determine the inherent ML/FT risk; any higher risk business is subjected to higher CDD and enhanced ongoing due diligence. Section 4 and Section 22 enforce the ultimate responsibility remains with the insurer when activities are outsourced or delegated and any such function is undertaken as if by the insurer instead of the service provider. The insurer must have procedures in place to meet the requirements of the Regulations including ensuring that activities or work carried out on its behalf are completed in compliance with the IAMLR Section 21, where reliance is placed by an insurer on an introducer to collect information and evidence of identity or any other form of CDD, Introduced business is addressed in detail in this report under Recommendation 9.

Effectiveness of implementation – R. 8

548. Specific requirements to prevent the risk of use of technological developments for ML or FT purposes were only recently introduced at the time of the onsite visit (August 1, 2008 for FSC licenseholders and September 1, 2008, for IPA-related businesses), with a parallel requirement from December 18, 2008 in the AML Code 2008. On that basis, it was not realistic to conduct a meaningful assessment of the effectiveness of the implementation of the new requirement.

549. With regard to non face-to-face business, it was evident to the assessors from discussions with financial institutions that such business is the norm in the IOM and, therefore, in some cases appeared to be regarded as routine. While some institutions identified the business as inherently high-risk and indicated that, as a consequence, they conducted CDD measures (identification and verification, including of the beneficial owner) directly and until the point where certainty had been achieved, other institutions welcomed the availability from the authorities of concessions designed to ease the CDD burden and were open to making full use of facilities such as Suitable Certifiers and Eligible Introducers. This may indicate uneven standards of implementation across the financial sector and the assessors recommend that this area should be a focus for additional supervisory attention by the regulatory authorities.

3.2.2. Recommendations and Comments

R.5

- The authorities should take steps to eliminate any residual inconsistencies in AML/CFT legal requirements and terminology.

- The authorities should expand the current list of categories of higher-risk customers and consider including, for example, private banking and business involving trusts or other legal arrangements.

- The authorities should conduct a risk-based review of the current scope of the Acceptable Applicant facility and, if warranted, limit its availability for consistency with the FATF Recommendations. To comply with the FATF Recommendations, financial institutions should be required in all cases to determine whether a customer is acting on behalf of another person and to take reasonable steps to obtain sufficient identification data to verify the identity of that other person.

- If the exceptions to the CDD requirements of secondary legislation as currently set out in the FSC Handbook are to be retained, the authorities should amend the secondary legislation as necessary to provide for them.

- Should the authorities decide to continue allowing source of funds to be used as principal evidence of identity in certain low-risk circumstances, the requirements should be tightened further to eliminate any remaining risk of abuse for ML or FT purposes.

- The authorities should review on a risk basis the implementation of the concession allowing operations to commence prior to completion of full CDD procedures to ensure it is not being misused.

- The authorities should ensure that insurance managers and insurance intermediaries are included within the scope of all relevant AML/CFT requirements.

R.8

- To support the implementation of the basic requirement in this area, the authorities should issue more detailed guidance on the specific ML and FT risks of new technologies, for example in relation to e-money and e-commerce.

3.2.3. Compliance with Recommendations 5 to 8

	Rating	Summary of factors underlying rating
R.5	**PC**	• Available concessions from conducting full CDD represent an overly-generous implementation of the FATF's facility to apply reduced or simplified measures, including where the customer is acting on behalf of another person. Financial institutions not required in all cases to determine whether a customer is acting on behalf of another person and take reasonable steps to obtain sufficient identification data to verify the identity of that other person. • Current list of suggested high-risk customers omits some significant high risk business categories relevant in the IOM. • Some residual inconsistencies and potential overlap/conflict between pieces of AML/CFT secondary legislation. • Some exceptions to CDD requirements provided for only in guidance. • As they were recently introduced at the time of the on-site visit, the effectiveness of implementation of some CDD requirements, and of the supplementary provisions of the AML Code 2008, could not be fully assessed.
R.6	**C**	
R.7	**C**	
R.8	**LC**	• Limited evidence of special attention to specific ML and FT risks of new technologies, including in relation to e-money and e-commerce and no evidence of testing by the FSC of implementation by financial institutions of appropriate measures. • As they were recently introduced at the time of the on-site visit, the

		effectiveness of implementation of the requirements regarding the risk of misuse of technologies and the risk resulting from non face-to-face business relationships could not be fully assessed.

3.3. Third Parties And Introduced Business (R.9)

3.3.1. Description and Analysis

550. As noted, much of the financial business in the IOM is conducted on a non face-to-face basis for nonresidents. IOM banking, insurance, and other financial services products are marketed globally, including through business introducers. The potentially long distribution chain may increase the exposure of IOM financial institutions to misuse for ML and FT purposes, including through layering and structuring, as they are remote from the customer and face an additional challenge in identifying with confidence the ultimate beneficial owner(s) or controller(s).[37] The IOM authorities developed a protocol to accommodate the use of business introducers by IOM entities subject to the AML Code 2008. Additionally, they have provided for a defined class of introducer (generally known as 'Eligible Introducer'), by availing of the provisions of FATF Recommendation 9 as a means of fulfilling the CDD obligations of Recommendation 5. The stated objective is to eliminate duplication of effort and documentation in cases that meet a set of conditions set out in secondary legislation and developed further in guidance. In addition to assessing formal compliance with Recommendation 9, the analysis below considers whether the protocol is sufficiently robust and implemented effectively to adequately control such additional risks as arise from reliance on third parties in conducting and documenting the necessary CDD procedures.

551. AML Code 2008 paragraph 11 sets out the basis on which CDD measures should be applied where business is introduced by a third party. It also defines the class of introducer commonly known as an 'eligible introducer' and sets out the eligibility criteria to permit reliance on them by IOM financial institutions and other relevant persons. The provisions are analyzed below for consistency with the criteria of Recommendation 9.

Requirement to Immediately Obtain Certain CDD elements from Third Parties (c. 9.1):

552. In the case of introduced business in general, pursuant to AML Code 2008 paragraph 11(4), the IOM financial institution or other relevant person is required to establish, maintain, and operate procedures that include:

(a) The production by the introducer of evidence of the identity of the applicant for business; or

(b) The taking of such other measures as will produce evidence of their identity;

[37] The risks arising from this type of business were discussed in the FATF Typologies Report 2004-5.

in each case in accordance with AML Code 2008 paragraph 6(3) which includes requirements to verify identity, obtain information on the purpose and intended nature of the business relationship; and taking reasonable steps to establish the source of funds.

553. It is not provided expressly in the Code or elsewhere that the evidence of identity should be provided to the IOM financial institution but this is understood by the requirement for 'production'.

554. With regard to business introduced by third parties pursuant to paragraph 11(4), the obligation to conduct CDD remains directly with the IOM financial institution in accordance with paragraph 11(3) and they may only rely on the introducer to source information and documentation on their behalf from the (prospective) customer and, as appropriate, the beneficial owner. This ultimate responsibility is emphasized in guidance issued to the institutions they regulate by the FSC and is also set out as a requirement for insurers in Sections 4 and 21(5) of the IAMLR.

555. By contrast, under paragraph 11(5), there is an exemption from the requirement to produce verification of identity in respect of business introduced by a third party if:

a) The relevant person has identified the applicant for business and the beneficial owner and knows the nature and intended purpose of the relationship; and

b) The introducer meets the definition of an 'eligible introducer', as set out below:

556. While the term 'eligible introducer' is not to be found in either the AML Code 2008 or the IAMLR 2008, it is included for convenience and for clarity in the following analysis as it is commonly used in practice in the IOM to refer to an introducer that meets the definition in AML Code 2008 paragraph 11(5)(c) (i), as follows:

a) a regulated person (defined in paragraph 2 of the Code to include specified categories of regulated financial institutions and fiduciaries in the IOM; specifically: banks, investment businesses, building societies, CSPs, TSPs, trustees of retirement benefit schemes, and retirement benefits scheme administrators);

b) an advocate or legal practitioner within the meaning of the Legal Practitioners Registration Act 1986 or an accountant carrying out business in or from the IOM, where subject to rules of a professional body that include requirements and procedures at least equivalent to the Code;

c) a person who acts in the course of external regulated business (defined in paragraph 2 of the Code to mean a regulated business outside the IOM that corresponds to any of those businesses regulated by the FSC or IPA) and which is regulated under the law of a country in the list in Schedule 2 to the Code (in which the IOM authorities have listed jurisdictions which, in their view based at least in part on published AML/CFT assessment reports, adequately apply the FATF Recommendations).

557. A number of issues arise with respect to the scope of the above definition:

- While the inclusion of certain IOM-regulated DNFBPs (specifically CSPs and TSPs) within the potential scope of the concession may appear justifiable, as noted in section 4 of this

report, the AML/CFT measures for a number of relevant categories of DNFBP in the IOM are still in the course of development and implementation. The current scope of AML Code 2008 could be misinterpreted as already granting the concession without regard to the enhancements still needed in AML/CFT coverage.

- While measures are already in place at least to some degree for IOM advocates, as noted elsewhere in this report there is no basis (and no proposal at the time of the assessment to introduce a basis) for applying or supervising the implementation of AML/CFT measures for non-IOM legal practitioners registered to conduct certain business in the IOM. Yet it would appear that the Eligible Introducer concession could apply in their case, albeit subject to the external regulated business test.

- A basis for the application of AML/CFT measures to IOM accountants based on membership of specific professional bodies had not been finalized at the time of the on-site visit; the pattern of application of AML/CFT measures to accountants in other countries is uneven and AML Code 2008 could be misinterpreted as granting the concession to them just by virtue of membership of professional bodies.

- The scope of the definition of external regulated business is broad and imposes a challenge (and therefore a heightened risk) for IOM institutions to determine accurately the extent of supervision to which the external regulated businesses are subject and whether or not that supervision adequately addresses AML/CFT matters.

558. To comply with the criteria of Recommendation 9, financial institutions must be required to obtain immediately the necessary CDD information from the third party and, with regard to business introduced by third parties in general, AML Code 2008 paragraph 11(2) provides that the production of satisfactory evidence of identity (or other equivalent measures) shall be undertaken before entering into a business relationship. Based on interviews with IOM financial institutions, the assessors formed the view that the (somewhat more liberal in terms of timeframe) requirement in place at the time of the on-site visit was being interpreted in some cases by financial institutions in a manner not fully consistent with the terms of Recommendation 9. The scope for deferred CDD has subsequently been removed by the authorities. While this post-visit strengthening of the requirements is to be welcomed, the assessors did not have the opportunity to confirm the effectiveness of implementation of the new measures.

559. For business sourced from eligible introducers, the requirement to verify identity may be waived provided that the financial institution has identified the applicant for business and beneficial owner; knows the nature and intended purpose of the relationship; and confirms that the eligibility criteria for introducers are met.

560. While insurers are subject to AML Code 2008, they are also covered by the IAMLR 2008 which sets out the basis on which the insurers can accept business sourced through introducers. A potential exception could arise in the case of entities such as insurance managers or insurance intermediaries because, as noted above, they do not come within the scope of the IAMLR 2008, but are covered by the Code. In relation to insurance business, where the insurance manager is managing an element of an IOM-regulated insurers' business then the IOM-regulated insurer is obliged to comply or be satisfied that the insurance manager is complying. In the event that an insurance

intermediary, regulated by the IPA, introduces its client to an IPA-regulated general insurer, than such insurer is subject to the full range of AML/CFT requirements. Insurance intermediaries of long term insurance business are regulated by the FSC and as such are subject to the FSC Rulebook.

561. Pursuant to IAMLR 2008 Section 9, an insurer must take reasonable measures to verify client identity and satisfy itself on the source of wealth and source of funds. The insurer must hold either original documents or suitably certified copies on its files, or undertake a form of investigation which satisfies the insurer in relation to client identity; the information must be reliable, independent source documents, data, or information. Such information may be obtained from an introducer, as defined in the IAMLR 2008 Section 21 and IGN 2008 Section 7. The introducer is not permitted to certify CDD documentation unless classified as a suitable certifier. Where an insurer is relying on an introducer to collect information and evidence of identity or any other form of CDD and permits the introducer to retain the information, such information and relevant identification data must be made available to the insurer 'upon request and without delay' pursuant to IAMLR Section 21.

562. Under the IGN 2008, the use of an Introducer's Certificate is permissible, defined in Section 12(i) as a document "which historically was an acceptable method of regulated introducers certifying the identity of an applicant without providing certified copy documents". Pursuant to Section 8, an IPA regulated entity can only accept, among other requirements, an Introducer Certificate if the introducer is regulated in a jurisdiction listed in Schedule 2 of the AML Code 2008. The assessors were advised during meetings with the industry and the authorities that Introducer Certificates are either no longer accepted by insurers or their use is no longer common practice (according to the IPA, currently used by only one insurer and only then from UK FSA-authorized and regulated intermediaries).

563. IAMLR 2008 Section 8 provides that the production of satisfactory evidence of identity (or other equivalent measures) shall be undertaken as soon as is reasonably practicable after the applicant applies to enter into a business relationship. In the event that the business relationship commences prior to the completion of the CDD process, the insurer must apply measures to control the type and volume of transactions that must be performed. While this provision may be pragmatic particularly for non face-to-face business, it does not equate to a requirement to obtain information immediately. However, as noted, AML Code 2008 paragraph 11(3) introduced a requirement for identification before entering into a business relationship, which is consistent with Recommendation 9.

Availability of Identification Data from Third Parties (c. 9.2):

564. AML Code 2008 paragraph 11(7) provides that financial institutions and other relevant businesses may not enter into a business relationship with a person introduced to them by a third party unless written terms of business are in place. Paragraph 11(7)(e) requires that such terms of business must require the introducer to supply to the relevant party forthwith upon request copies of the evidence verifying the identity of the applicant for business and of the beneficial owner and all other CDD data held by the introducer. Similarly, for insurance businesses, IAMLR 2008 Section 21 provides that regulated entities may not enter into a business relationship with an introducer unless written terms of business are in place. Section 21(3) requires that such terms of business must require the introducer to supply forthwith upon request the evidence verifying the identity and all other related CDD of the applicant and of the beneficial owner or controller who exercises influence over the policyholder.

Regulation and Supervision of Third Party (applying R. 23, 24 & 29, c. 9.3):

565. AML Code 2008 paragraph 11(8) places responsibility on the relevant person to ensure that the procedures of the introducer are fit for the purpose of ensuring that evidence produced, or to be produced, is satisfactory and that the procedures of the introducer are also fit for that purpose. Paragraph 11(9) of the Code requires that a relevant business must randomly test these procedures to satisfy itself that procedures for compliance with these requirements are sufficiently robust and effective. An explicit requirement has been introduced in paragraph 11(10) in compliance with Recommendation 9 that financial institutions satisfy themselves that the introducer is regulated and supervised for AML/CFT purposes and also requires the taking of steps as necessary to ensure awareness of any material change to the intermediary's status or of that of the jurisdiction in which the introducer is regulated. This represented a significant strengthening of the IOM requirements.

566. Pursuant to IAMLR 2008 Section 21(2), IPA-regulated entities must ensure that the ongoing monitoring of an introducer includes information on the introducer's regulatory status. However, it appears that an adequate regulatory status might not be a prerequisite for entering into an agreement with an introducer as IGN 2008 Section 7.4 outlines a procedure that insurers could apply in assessing regulatory status and the regulatory body. Under Section 7.5, an insurer must have in place procedures to monitor the ongoing status of all regulated introducers who hold customer due diligence documentation on its behalf, and also undertake sample testing to ensure that the documents can be retrieved when required and that the regulated introducer has measures in place to comply with the CDD requirements.

Adequacy of Application of FATF Recommendations (c. 9.4):

567. In compliance with Recommendation 9, AML Code 2008 paragraph 11(6) excludes from the scope of the 'Eligible Introducer' concession introducers from any country that does not apply or insufficiently applies the FATF Recommendations in respect of the business of the introducer.

568. While IGN Section 7.4 require insurers to consider the location, regulatory status, and regulatory body of the introducer when determining whether the procedures of the introducer are fit for purpose, no specific requirement exists for considering whether the introducer's jurisdiction adequately applies the FATF Recommendations. IGN 7.4 provides that when an insurer has reason to believe that an introducer is subject to insufficient ML/FT regulation, the insurer may wish to introduce additional measures, including but not limited to devising CDD procedures for the introducer to undertake. These additional measures are not mandatory and are at the discretion of the insurer.

Ultimate Responsibility for CDD (c. 9.5):

569. In line with Recommendation 9, AML Code 2008 paragraph 11(13) provides that the ultimate responsibility for ensuring that CDD procedures comply with the terms of the Code remains with the relevant person. For FSC-regulated entities, clarification is also provided in the FSC Handbook Sections 4.11 and 4.12 that responsibility remains with the IOM licenseholder.

570. For IPA-regulated insurers, IAMLR Section 9(4) prohibits delegation of responsibility for CDD. Responsibility remains with the insurer for outsourcing or delegated functions to 'ensure that

the activities or work carried out on its behalf are completed in accordance with these Regulations, and that adequate procedures are in place which meet the requirements of these Regulations'. While IGN Section 2.5 permits reliance to be placed on the information collected by the third party, pursuant to Section 7.1, the ultimate responsibility for CDD and verification remains with the insurer. As noted in Section 3.2 of this report, IPA regulated insurers need to comply with two pieces of secondary legislation being the AML Code 2008 and the Insurance (Anti-Money laundering) Regulations 2008 and a question could arise as to which takes legal precedence in cases where the legislative provisions overlap or conflict.

Effectiveness of implementation

571. In practice, introducers represent an important source of new and continuing business for IOM financial institutions. The assessors found that a range of approaches is employed by financial institutions in determining whether and, if so, the extent to which they place reliance on the Eligible Introducers to conduct CDD on their behalf, beyond merely using them to source CDD information. Some financial institutions place reliance on Eligible Introducers to the full extent permitted. Others are more selective, working with a smaller sub-set of known and trusted introducers of a particular type and/or in specific jurisdictions. For some, corporate policy requires that all CDD procedures must be conducted directly by staff of the IOM financial institution; while others have learned from unsatisfactory past experiences and no longer rely on the introducers.

572. Among the factors which may undermine the effectiveness of implementation of the concession is the difficulty that may arise in determining whether a foreign introducer is, in reality, regulated and supervised specifically for AML/CFT purposes (rather than for prudential or market practice purposes), particularly given the wide definition of external regulated business in AML Code 2008 Section 2.

573. While it is difficult to form a definitive view regarding the overall quality of implementation, there were strong indications during the assessment that the operation of the Eligible Introducer arrangement was not without significant reputational risk to the IOM, with anecdotal evidence of significant deficiencies in some cases, which contrasted with a high level of reported satisfaction with the quality of the information provided by introducers in other cases. The regulatory authorities provided the assessors with evidence that they take into account the inherent risks and give considerable attention to introduced business as part of their on-site work. It is an area on which regulatory authorities should continue to focus particular attention as part of their onsite inspection programs.

3.3.2. Recommendations and Comments

- The authorities should review the range of business introducers in respect of which concessions are applied to ensure that all categories are subject to equivalent AML/CFT requirements.

- By means of on-site supervision or otherwise, the regulatory authorities should assess the effectiveness of CDD being obtained from Eligible Introducers or Introducers including, in the case of insurers, the use and effectiveness of Introducer's Certificates.

- The authorities should remove any residual inconsistencies in secondary legislation following the coming into force of the AML Code 2008.

3.3.3. Compliance with Recommendation 9

	Rating	Summary of factors underlying rating
R.9	**LC**	• Not all permitted categories of introducer were subject to full AML/CFT requirements. • Indications of inconsistent implementation by financial institutions in relation to requirements in place at the time of on-site visit in applying due diligence relating to their reliance on Eligible Introducers, introducers, or Introducer's Certificates, as applicable.

3.4. Financial Institution Secrecy or Confidentiality (R.4)

3.4.1. Description and Analysis

Inhibition of Implementation of FATF Recommendations (c. 4.1):

574. There are no statutory financial institution secrecy provisions under IOM law that would inhibit the implementation of the FATF Recommendations. There is, however, strict application by financial institutions of the common law duty of confidentiality in respect of their client information. For specified purposes, including for purposes of financial sector supervision and AML/CFT, statutory provisions override the common law duty of confidentiality subject to strict safeguards. Provisions relevant to AML/CFT include:

- Sections 17K CJA 1990, 48 DTA 1996, and 11 ATCA 2003, which make it an offense not to report knowledge or suspicion that a person is engaged in laundering the proceeds of criminal conduct and are the principal powers under which financial institutions report suspicions to the FCU. This topic is analyzed in detail in the assessments of R.13 and elsewhere in section 2 of this report, including the powers of the law enforcement agencies and the FCU in particular to gain access to confidential client information for purposes of their investigations. In brief, a Court order ('production order') or warrant is required for such access, thus overriding the duty of confidentiality.

- While there is no secrecy law preventing financial institutions from providing information to each other where necessary for AML/CFT purposes, at the time of the onsite visit there also was no specific provision in place that would explicitly override the duty of confidentiality and thus empower financial institutions to exchange such information for purposes of R.7, R.9, or SR.VII. This matter is to be addressed in Section 147 POCA (2008) which had not come into force at the time of the assessment. In practice, however, financial institutions did not identify to the assessors any confidentiality-related difficulties in exchanging information between themselves for AML/CFT purposes when the exchange is conducted in accordance

with normal industry practices or in the course of meeting their CDD requirements.

575. With regard to access by relevant (including supervisory) authorities to confidential information held by financial institutions, relevant provisions are contained in the FSA 2008, which came into effect on August 1, 2008 and largely replicates legislative provisions under earlier supervisory legislation. The provisions include:

- Section 15 FSA 2008 bringing into effect Schedule 2 FSA 2008 which lists the FSC's powers to inspect books, accounts, and documents of financial institutions; to require the provision by financial institutions of such information as the FSC may reasonably require for the performance of its functions under the FSA 2008 (which includes explicitly as a regulatory objective in Section 2 (2)(c) FSA 2008 'the reduction of financial crime'); to enter property and take possession of documents; and other powers to require the appointment of reporting accountants or appoint an external inspector to provide the FSC with a report on any matter relevant to the supervision of a financial institution under FSC supervision.

- Section 34 FSA 2008 which empowers the FSC to enter into mutual assistance agreements with regulatory authorities (as defined in Section 48 FSA 2008 to apply to a broad categories of regulatory or supervisory authority in the IOM or otherwise). Section 34(3) FSA 2008 empowers the FSC to conduct an investigation on behalf of another regulatory authority where requested by that authority for purposes of assisting it in the exercise of its functions. The exercise by the FSC of its powers under these provisions is subject to specific limitations: Section 34(4) FSA 2008 provides that the above provisions "shall not permit the disclosure of any information relating to the affairs of a customer other than in accordance with Schedule 5" FSA 2008. Schedule 5 contains a complex set of provisions limiting the provision of customer information to ensure that such information may be used only in accordance with regulatory powers and for valid purposes. Unless the approval of the customer is obtained before information is provided to the foreign authority, the information is subject to certain controls on its use and dissemination. The published policy of the FSC, including as signatory of the IOSCO MMOU, is to provide full and timely assistance to other regulators. This issue is addressed further in the analysis in this report of compliance with R.40.

576. In relation to relevant provisions including supervisory actions vested in the IPA, the IA 2008 Schedule 5 enables the IPA to exercise its powers to inspect the books, accounts, and documents and to undertake such inspections and investigations in relation to the concerned insurer, pursuant to Schedule 5: an insurer or former insurer; a person suspected of or appearing to carry on contracts of insurers; a controller including a body corporate; any associate or former associate; any partnership; customers or former customers; and any other person with whom the insurer had formed a business relationship. Such powers include the power of entry and access.

577. The exercise by the IPA of its powers under these provisions is subject to specific limitations: Schedule 6 IA 2008 provides that, under the above provisions, the IPA shall treat information relating to the business or other affairs as restricted and shall not disclose such information other than in relation to the exceptions listed in Schedule 6.2. Schedule 6.1 does not preclude the disclosure of information to a recognized regulator, whether a governmental or private body, in the IOM or

elsewhere, for the purposes of discharging its functions and to exercise such functions relating to financial crime pursuant to Section 37 and Schedule 6.2(2) IA 2008.

578. The IA 2008 Schedule 5 largely replicates the powers conferred on the IPA under IA 1986 and further extends inspection and investigative powers specifically to registered or former insurance intermediaries; managers; persons exempt from registration; any scheme or former scheme including administrators or trustees to such schemes; and to 'any person who the Supervisor has reason to believe has information that is relevant to the discharge of the Supervisor's functions under the Act' on reasonable grounds.

3.4.2. Recommendations and Comments

- Bring into force the provision that financial institutions do not breach their confidentiality duty in exchanging customer information between themselves for AML/CFT purposes.

3.4.3. Compliance with Recommendation 4

	Rating	Summary of factors underlying rating
R.4	**LC**	• Explicit exclusion from common law duty of client confidentiality not yet brought into force to permit financial institutions to exchange information.

3.5. Record keeping and wire transfer rules (R.10 & SR.VII)

3.5.1. Description and Analysis

Legal Framework:

579. Record keeping requirements applicable to financial institutions and other relevant persons are set out in the AML Code 2008, paragraph 4(1)(a)(ii) of which provides that they must establish, maintain, and operate record keeping procedures in accordance with paragraphs 16–19, dealing respectively with: records of verification of identity; records of transactions; retention of records; and their format and retrieval. For FSC-regulated entities, further requirements are set out in FSC Rule Book 2008 Rule 9.16, supported by detailed guidance in the Handbook 2008.[38]

580. More broadly, in terms of accounting records, under the Banking Act 1998, Code 78 of the Banking (General Practice) Regulatory Code 2005 requires a licenseholder to keep such accounting records as are necessary to accurately disclose its business transacted in or from the IOM at any time. Such records must be maintained for a period of six years. For IPA-regulated insurers, record keeping

[38] The authorities pointed out that, prior to the FSC Rule Book 2008, the record keeping requirements for fiduciaries were set out in the Fiduciary Services (General Requirements) Regulatory Code 2005 and for investment businesses in the Financial Services Commission (Financial Resources and Compliance Reporting) Regulatory Code 2002.

requirements are set forth in IAMLR 2008 Regulations 28–30 and further detailed requirements are contained in the IGN 2008.

Record-Keeping & Reconstruction of Transaction Records (c. 10.1 & 10.1.1):

581. In accordance with Recommendation 10, pursuant to AML Code 2008 paragraphs 16 and 17(1), financial institutions and other relevant persons must, for at least five years from the date of the transaction, keep records of all transactions carried out, including identification data, account files, business correspondence records, and records sufficient to permit reconstruction of individual transactions and compliance with the Code. As no distinction is made between domestic or international transactions or based on whether the business relationship is ongoing or has been terminated, the requirement applies to records of all transactions. In respect of insurers, Regulation 29 of the IAMLR 2008 further requires 'that records be maintained for at least five years from the date of the last transaction or when the business relationship was formally ended' and therefore, in this instance, distinction is made between whether the business relationship is ongoing or has been terminated.

582. With effect from December 18, 2008, AML Code 2008 paragraph 17(3) introduced an explicit provision that, where a relevant person becomes aware that a request for information or an enquiry is underway by a competent authority, all relevant records must be maintained for as long as required by the competent authority. For FSC-regulated entities, Section 8 of the Handbook sets out details of the measures they are expected to have in place, albeit with the status of guidance.

583. An important issue in the case of the IOM, having regard in particular to the eligible introducer system, is the retention of records held on behalf of IOM financial institutions and other relevant persons by third parties, often from outside the IOM. AML Code 2008 paragraph 11(7) requires that record keeping in accordance with paragraph 17(1) shall be included in the written terms of business that must be in place with the eligible introducer, the enforcement of this aspect of the terms of business could present difficulties in practice in some jurisdictions. The authorities pointed out that the fact that records may be retained abroad does not exempt a financial institution from its statutory obligations in the IOM. Also, the risk of difficulties arising in information access is mitigated to some extent by the requirement under AML Code 2008 paragraph 11(9) for the testing, on a random and periodic basis, of the procedures (which would include those for the supply forthwith upon request of the evidence verifying the identity of the applicant for business and the beneficial owner in any particular case) with a view to ensuring their effectiveness. AML Code 2008 paragraph 18(2) tries to address the potential difficulties by requiring that introducer produce upon request copies of the records requested and notify should they be no longer able to comply with that requirement. Moreover, detailed requirements were introduced by means of AML Code 2008 paragraph 11(7)(f) and (h) to 'supply to the relevant person forthwith copies of' identification/verification evidence and all other CDD data where:

(a) The introducer is to cease trading;

(b) The introducer is to cease doing business with the applicant for business; or

(c) The relevant person informs the introducer that it no longer intends to place reliance on that introducer.

584. For FSC-regulated entities, FSC Rule Book Rule 9.16 restates the record-keeping requirements of the Code, though with some differences. Under Rule 9.16, in addition to making records available to a constable, requires that the records must also be available if required internally to staff of the licenseholder and to the FSC. Rule 9.10 also contains requirements for record keeping as part of the mandatory terms of business in relation to reliance on Eligible Introducers. Sections of the Rule Book other than Section 9 on AML/CFT also contain requirements on record keeping more generally. However, only Section 9 had been brought into force within the timeframe of this assessment, with the remainder of the Rule Book due to come into effect from January 1, 2009, and, being outside the timeframe of the assessment, are not analyzed further here.

585. IAMLR 2008 Regulations 28–30 require that records be maintained for at least five years from the date of the last transaction or when the business relationship was formally ended. Such records must be sufficient to:

- identify the source and recipient of payments to permit authorities and competent third parties to assess the insurer's observance of ML policies and procedures;
- compile an audit trail for the reconstruction of any transactions; and
- satisfy within a reasonable timeframe any enquiries or court orders as to the disclosure of information.

586. As with FSC regulated entities, no distinction is made between domestic or international transactions or based on whether the business relationship is ongoing or has been terminated: records of all transactions are required to be maintained.

587. Further, pursuant to IAMLR 2008 Regulation 29(2) where a report has been made to the FCU, or where the insurer should know or knows of a matter under investigation, the insurer must retain all records for as long as required by the FCU.

588. IGN 2008 expands on the record-keeping requirements, detailing the requirements pursuant to Section 10 including transaction records; compliance and money laundering reporting officer records; introducer records; and transaction records and documentation.

Record-Keeping for Identification Data, Files and Correspondence (c. 10.2):

589. In line with Recommendation 10, AML Code 2008 paragraph 16 requires financial institutions and other relevant persons to maintain records of identification data, account files, and business correspondence records for at least five years.

590. For FSC licenseholders, FSC Rule Book 2008 Rule 9.16 also requires the retention of all information resulting from any step taken in identifying, or verifying the identity of, or obtaining any information concerning any person or ascertaining the source of funds. As noted earlier, separate requirements addressing the maintenance of business and accounting records apply a mandatory minimum retention period of six years for some relevant records. Sections of the Rule Book other than Section 9 on AML/CFT also contain relevant requirements in this context. However, only

Section 9 had been brought into force within the timeframe of this assessment, with the remainder of the Rule Book in effect from January 1, 2009 and, therefore, outside the timeframe of this assessment.

591. For IPA-regulated insurers, all records prepared and maintained on its policyholder relationships and transactions must be retained for at least five years from the date of the last transaction or when the business relationship was formally concluded. As referred to above, the time frame can be extended as required by the FCU.

592. Pursuant to IAMLR 2008 Regulation 30, all CDD information must be available for investigative purposes 'wherever held, and whether held by the insurer or not'. IGN 2008 expands on the record-keeping requirements and pursuant to Section 10(2) all documents relating to CDD and all other functional areas that the insurer may be involved in at any stage in the duration of the insurance contract must be detailed and maintained, including any file notes and supporting documentation. Where records are maintained by a third party, including regulated introducers, the legal responsibility remains with the insurer to ensure the ability of retrieval and recreation of the transaction records. IGN 2008 Section 10.4 sets out requirements in relation to transaction records including origin of funds and the destination of funds. Section 10 requires insurers to advise all introducers of the applicable requirements of the AML Code 2008, IAMLR 2008 and IGN 2008.

593. Availability of Records to Competent Authorities in a Timely Manner (c. 10.3):

594. Provisions in relation to retrieval of records are set out in AML Code 2008 paragraph 18. If the records are in the form of hard copies kept in the IOM, the relevant persons must ensure that they are capable of retrieval without undue delay; if they are in the form of hard copies kept outside the IOM, they must ensure that the copies can be sent to the IOM and made available within seven working days; in the case of other records, including copies kept on a computer system, they must ensure that they are readily accessible in or from the IOM and that they are capable of retrieval without undue delay. There is also an obligation on the relevant persons if they rely on third parties, to ensure that they are satisfied that the third party is required upon request to produce copies of the records required and that the third party must notify the relevant person if no longer able to comply for whatever reason. In addition, AML Code 2008 paragraph 11(7)(d) requires that record keeping in accordance with paragraph 16 shall be included in the written terms of business that must be in place with an eligible introducer. These provisions aim to ensure that the appropriate records are available to the IOM licensed entity.

595. With regard to availability of the records to the IOM competent authorities, access for a constable (relevant for FCU and law enforcement purposes) was noted earlier. In addition, a number of methods are provided to allow access for the FSC to the records of its licenseholders under the FSA 2008, including the powers of inspection and investigation in Section 15 and Schedule 2, among which is the power to request information about the affairs of a customer (Schedule 2, Paragraph 2) and the power to issue direction (Schedule 2, Paragraph 2(3)). Paragraph 3 provides the FSC with powers to require information where authorized in writing by a Justice of the Peace, which is the method normally used by the FSC to obtain AML/CFT information for use in investigations.

596. For IPA-regulated entities, both the IAMLR 2008 and the IGN 2008 contain provisions that require an insurer to retrieve all records and satisfy, within a reasonable time, any court orders or enquiries from appropriate authorities requiring disclosure of information. No maximum time-line is

stipulated. Pursuant to IAMLR 2008 Regulation 28 (2), any records kept in electronic format must be available, legible, and capable of reproduction in a manner acceptable to the IPA and IOM Courts. IGN 2008 8.6 sets forth that insurers must have in place written procedures for obtaining copies of documentation from the introducer on request, both on an ad hoc basis or in the event of cessation of business.

597. The legal framework as described is in line with the international standard. There remains some risk that the information held by third parties might not be released in practice, particularly if held outside the IOM, despite the IOM licensed entity having been satisfied that no such difficulty would arise. The requirements introduced in this regard in late-2008 by the IOM authorities appear to go as far as it is possible to go to mitigate this risk, but it cannot be eliminated entirely as implementation remains to some extent beyond the control of the IOM-regulated entity.

Effectiveness of implementation – R.10

598. In practice, all financial institutions interviewed during the assessment confirmed that they retain all records of transactions, account opening and ongoing due diligence, accounts, and correspondence for at least five years, and more typically for 10 or 12 years. All records retained in the IOM are available to the relevant competent authorities without delay. The assessors noted that some financial institutions maintain part of their records at group facilities outside the IOM, mainly in the UK. With regard to dependence on third parties to maintain records and provide them swiftly upon request, some of the institutions interviewed expressed satisfaction with the service provided by eligible introducers and other third parties; others indicated concerns and had stopped availing of the facility to rely on third parties. The relevant competent authorities confirmed that they do not encounter difficulties or delays in obtaining the information and records they request from licenseholders and that they take care to select the appropriate legal channels and follow the set procedures in requesting information and records for investigative purposes.

Obtain Originator Information for Wire Transfers - Introduction:

599. Having regard to the fact that the IOM is in monetary union with the UK, following a request made to the EU by the UK Treasury on behalf of the IOM authorities, a derogation was approved on December 8, 2008 in respect of EU Regulation 1781/2006.[39] The derogation provides for the UK to establish agreements with Jersey, Guernsey, and the IOM so that the reduced information requirement can apply to payments passing between the UK and these associated territories. The derogation would not apply between that territory and any other Member State. The assessors understand that for the derogation to take full effect, a formal agreement is still required between the IOM and UK authorities, which was not in place within the timeframe of this assessment.[40] However, as the derogation has been approved by the EU Member States and all relevant documentation was available to the assessors, the derogation has been taken into account for purposes of this assessment.

[39] EU Regulation 1781/2006 implements SR.VII for all EU Member States.

[40] The agreement was since documented and awaiting signature in the UK.

600. Provisions in relation to wire transfers are set out, not in primary legislation, the AML Code 2008, or the FSC Rule Book 2008, but by order. The IOM authorities opted to implement European Regulation 1781/2006 on Wire Transfers with appropriate modifications by means of orders by the Council of Ministers which constitute secondary legislation in the IOM, the "European Community (Wire Transfers Regulation) (Application) Order 2007", as amended by the "European Communities (Wire Transfers Regulation) (Application) (Amendment) Order 2007". To mirror the EU sanctions for non-compliance and date of implementation the EC Wire Transfers Regulation (Enforcement) Regulations 2007 came into force on December 15, 2007. In Article 3 (entitled Scope) of EC Regulation 1781/2006, as applied in the IOM by the European Communities (Wire Transfers Regulation) (Application) (Amendment) Order 2007, the Regulations are not applied to credit/debit card transactions at paragraph 2. Payments between financial institutions whilst acting on their own behalf are excluded from the Regulations at paragraph 7(c) of the same Article 3.

601. Detailed guidance on the application of the wire transfer requirements is set out in the FSC Handbook 2008 Section 5.3. The Handbook clarifies that the Regulation is widely drawn and intended to cover all types of funds transfer falling within its definition as made 'by electronic means' other than those specifically exempted wholly or partially by the Regulation. For UK Payment Area[41] based payment system provides it includes, but is not necessarily limited to, international payment transfers made via SWIFT, including various EUR payment systems, and domestic transfers via the UK payment systems, CHAPS and BACS.

Obtain Originator Information for Wire Transfers (applying c. 5.2 & 5.3 in R.5, c.VII.1):

602. Payment service providers are required, before transferring funds other than from an account, to verify the complete information on the payer on the basis of documents, data, or information obtained from a reliable and independent source, where the amount exceeds EUR1,000 (or the transaction is carried out in several operations that appear to be linked and together exceed EUR1,000). The exemption threshold does not apply where there is a suspicion of money laundering. (European Regulation (Application) Order, paragraph 5.4).

603. Complete information on the payer is clarified in the Handbook Section 5.3.4.1 to consist of name, address, and account number. A number of exceptions are permitted in the IOM consistent with the terms of SR.VII and are used in practice by the banks. For example, as a substitute for the address information, the Handbook specifies that the payer's date and place of birth, or national identity number, or customer identification number may be substituted. In the event that the recipient bank demands the payer's address where one of the alternatives had initially been provided, only with the payer's consent or under judicial compulsion would the address be additionally provided. Where the payment is not debited to a bank account, the requirement for an account number must be substituted by a unique identifier which permits the payment to be traced back to the payer. One of the IOM banks interviewed during the assessment indicated that, as a matter of practice, they chose to use unique identifiers for wire transfers generally.

Inclusion of Originator Information in Cross-Border Wire Transfers (c. VII.2):

[41] UK, Jersey, Guernsey, and the IOM.

604. Chapter II, Article 5, paragraph 1 of EC Regulation 1781/2006, as applied in the IOM by the European Communities (Wire Transfers Regulation) (Application) (Amendment) Order 2007 requires the full originator information to accompany a wire transfer of the required amount. The SR.VII concession relating to batch file transfers is applied in accordance with the international standard pursuant to Chapter II, Article 7, paragraph 2 of EC Regulation 1781/2006, as applied in the IOM by the European Communities (Wire Transfers Regulation) (Application) (Amendment) Order 2007.

605. Where the banks of both payer and payee are located within the UK Payment Area (defined in the IOM as equivalent to domestic), wire transfers need be accompanied not by full originator information but only by the payer's account number or by a unique identifier which permits the transaction to be traced back to the payer. However, if requested by the payee's bank, complete information must be provided by the payer's bank within three working days. On December 8, 2008, the European Commission confirmed the agreement of Member States to grant a derogation for the IOM for UK Payment Area wire transfers.

Inclusion of Originator Information in Domestic Wire Transfers (c. VII.3):

606. As noted, the IOM provisions define domestic transfers as including those to/from the UK Payment Area. Financial institutions have to comply with VII.2 above as per Chapter II, Article 5, paragraph 1 of EC Regulation 1781/2006, as applied in the IOM by the European Communities (Wire Transfers Regulation) (Application) (Amendment) Order 2007 except where the concession at Chapter II, Article 6 applies. As explained above, the required details must then be supplied within three working days if requested to do so.

607. Clarification of the position of the EU Member States having been obtained, the IOM definition of domestic can be accommodated within the current interpretation of the FATF Recommendations.

Maintenance of Originator Information (c.VII.4):

608. Banks must have systems in place to detect when the originator information is incomplete or missing pursuant to Chapter III, Article 8 of EC Regulation 1781/2006, as applied in the IOM by the European Communities (Wire Transfers Regulation) (Application) (Amendment) Order 2007. If such wire transfers are detected the details must be requested, or the transfer rejected, as per Chapter III, Article 9 of the same Regulation. Intermediary payment service providers are required to ensure that all information received on the payer that accompanies a transfer of funds is kept with the transfer as per Chapter IV, Article 12 of EC Regulation 1781/2006, as applied in the IOM by the European Communities (Wire Transfers Regulation) (Application) (Amendment) Order 2007.

609. The requirements regarding how to proceed when systems have technical limitations and the requirements to keep subsequent records for five years are detailed at Chapter IV, Article 13 of EC Regulation 1781/2006, as applied in the IOM by the European Communities (Wire Transfers Regulation) (Application) (Amendment) Order 2007.

Risk Based Procedures for Transfers Not Accompanied by Originator Information (c. VII.5):

610. The FSC Handbook 2008 clarifies that banks must have effective procedures for checking that incoming wire transfers are compliant with the relevant information requirement, as explained below. In order not to disrupt straight-through processing, it is not expected that monitoring should be undertaken at the time of processing the transfer. The Regulation specifies that banks should have procedures "to detect a lack of presence" of the relevant information, which is a reference to the validation rules of whichever messaging or payment system is being utilized. Additionally, the Regulation requires banks to take remedial action when they become aware that an incoming payment is not compliant. The payment service provider in such circumstances is required to adopt a risk-based approach and take it into account when assessing if such a wire transfer is suspicious and whether to make a report to the FCU. The requirement is at Chapter III, Article 10 of EC Regulation 1781/2006, as applied in the IOM by the European Communities (Wire Transfers Regulation) (Application) (Amendment) Order 2007. Hence, in practical terms it is expected that this requirement will be met by a combination of the following: Licenseholders must therefore subject incoming payment traffic to an appropriate level of post event random sampling to detect non-compliant payments. This sampling should be risk based, explained in the Handbook as follows:

(a) the sampling could normally be restricted to payments emanating from banks outside the UK Payment Area where the complete information requirement applies;

(b) the sampling could be weighted towards non-FATF member jurisdictions, particularly those deemed high risk under a bank's own country risk assessment, or by reference to external sources such as Transparency International, or FATF or IMF country reviews;

(c) focused more heavily on transfers from those Payer banks are identified by such sampling as having previously failed to comply with the relevant information requirement;

(d) other specific measures might be considered, e.g., checking, at the point of payment delivery, that payer information is compliant and meaningful on all transfers that are collected in cash by payees on a "Pay on application and identification" basis.

(e) None of the above requirements obviate the obligation to report suspicious actions in accordance with normal suspicious transaction reporting procedures.

611. In practice, the assessors received mixed responses from IOM banks regarding their treatment of incoming wire transfers that lacked full originator information. Additional clarifications were received on this issue from the authorities and some banks subsequent to the on-site visit. The banks confirmed that they apply a risk-based approach in considering whether further action is warranted to address the absence of full originator information. As an indicative example, one bank provided evidence that it systematically reviews incomplete wire transfer receipts from a set of high-risk countries (as defined by the particular financial services group) and may request additional information from the sending bank if the transaction cannot be explained within the bank. For countries of origin not on this list of jurisdictions, a 10 percent sampling rate is applied. A list is maintained of 'frequent offenders' with regard to failure to provide complete originator information and such banks are contacted and improvement requested; the assessors understand that these controls are implemented primarily at UK group level. Overall, while the measures in place in IOM banks

could be interpreted as within the risk-based terms of SR.VII, they represent only a partial application of the objective that obtaining originator information is the expected standard procedure, with exceptions acceptable only in low-risk circumstances.

612. Some smaller IOM banks, without direct access to wire-transfer facilities, contract with larger IOM banks (typically subsidiaries of UK clearing banks) to transmit payments on their behalf. Based on information provided to the assessors, it appeared that there were difficulties in some cases in arranging to have full originator information on the payer (customer of the smaller IOM bank) transmitted successfully to and through the IOM intermediary bank.

613. The requirement to restrict future business and to take other appropriate action such as terminating the relationship, plus making report to the FSC, is at Chapter III, Article 9, paragraph 2 of EC Regulation 1781/2006, as applied in the IOM by the European Communities (Wire Transfers Regulation) (Application) (Amendment) Order 2007.

Monitoring of Implementation (c. VII.6):

614. The FSC does not routinely monitor implementation of the wire transfer provisions as, to date, it has not been viewed as a higher risk issue but plans to do so as part of the visit cycle process in 2009/10. In practice, most of the IOM's banks are branches or subsidiaries of banks in the EU and group procedures are applied. This reliance on group procedures is not fully in compliance with the monitoring requirements of SR.VII.

Application of Sanctions (c. VII.7: applying c.17.1 – 17.4):

615. Sanctioning powers as set out in the analysis of Recommendation 17 apply also in relation to wire transfers, pursuant to the EC Wire Transfers Regulation (Enforcement) Regulations 2007 Sections 3 and 5(1–3). Under Section 43 of the FSA 2008, if an FSC licenseholder is in contravention of any statutory provision, the FSC may exercise any power that is an action for breach (but with the exception of the powers under Section 16 and Section 20 of the Financial Services Act 2008). Actions for breach are defined in Section 48 of the Financial Services Act 2008 and include revocation of suspension of a license, issue of directions in respect of an individual's fitness and propriety and service of warning notices.

Additional elements: elimination of thresholds (c. VII.8 and c. VII.9) (c. VII.8 and c. VII.9):

616. IOM law does not require incoming or outgoing wire transfers under EUR/USD1,000 to contain full originator information.

3.5.2. Recommendations and Comments

SR.VII

- The FSC should reconsider whether the current implementation of the risk-based approach for incoming wire transfers lacking full originator information accurately reflect the level of underlying risk.

- The FSC should continue to include wire transfers within its program of on-site supervision.

3.5.3. Compliance with Recommendation 10 and Special Recommendation VII

	Rating	Summary of factors underlying rating
R.10	**C**	
SR.VII	**LC**	• Tighter implementation may be needed in applying the risk-based approach when dealing with wire transfers that lack full originator information. • Need for additional FSC monitoring of ongoing compliance with wire-transfer requirements.

3.6. Monitoring of Transactions and Relationships (R.11 & 21)

3.6.1. Description and Analysis

Special Attention to Complex, Unusual Large Transactions (c. 11.1): Examination of Complex & Unusual Transactions (c. 11.2):

617. Financial institutions and other relevant persons are required, pursuant to AML Code 2008 Paragraph 7 which addresses continuing business relationships, to establish, maintain, and operate specified procedures in relation, inter alia, to:

- A suspicious pattern of transactions;

- Transactions or patterns of transactions that are complex or unusually large and which have no apparent economic or visible lawful purpose; or

- Unusual patterns of transactions which have no apparent economic or visible lawful purpose. (paragraph 7(2) (b), (c) and (d))

618. The procedures required pursuant to AML Code 2008 paragraph 7 include an examination of the background and purpose of the transaction or circumstances and, where necessary, reidentification of the customer or beneficial owner.

619. A new provision was introduced in AML Code 2008 paragraph 9(6) to require a relevant person to take adequate measures to compensate from any risk arising from one-off transactions that are complex or unusually large or have no apparent economic or visible lawful purpose. In addition, the FSC Rule Book and IAMLR address all relevant elements for FSC licenseholders and IPA-licensed insurers, respectively. Paragraph 15 of the AML Code 2008 also contains requirements for all relevant persons to perform ongoing monitoring, including scrutiny of transactions and other activities, paying particular attention to transactions that are complex, large, or unusual, or of an unusual pattern, and which have no apparent economic or lawful purpose.

620. For FSC-regulated entities, FSC Rule Book Rule 9.15 requires licenseholders to perform ongoing and effective monitoring, including appropriate scrutiny of transactions and other activities, paying particular attention to those defined in Recommendation 11. The extent and frequency of monitoring must be determined on the basis of materiality and risk, consistent with the risk assessment required under Rule 9.4 and by reference to Rule 9.9 which provides the basis for enhanced due diligence. Rule 9.15(3) requires enhanced measures for non face-to-face business.

621. For IPA-regulated insurers, IAMLR Section 17 provides that insurers must pay special attention to 'complex transactions; unusual large transactions; unusual patterns of transactions; and transactions with no apparent visible economic or lawful purpose', both at the inception of the business relationship and during its lifetime. Insurers must maintain a written record of the results of their examination of the background and purpose of such transactions.

Record-Keeping of Findings of Examination (c. 11.3):

622. Pursuant to AML Code 2008 paragraph 7(3), financial institutions and other relevant persons undertake 'an examination of the background and purpose of the transactions or circumstances' for the categories listed in paragraph 7, which includes transactions that have no apparent economic or visible lawful purpose. Under paragraph 7(4), in line with Recommendation 11, they must also keep written records of any examination, steps, measures, or determination made or taken and, on request, provide the findings to the competent authorities and auditors. Records required by the Code must be retained for at least five years (paragraph 17(1)).

623. For FSC licenseholders Rule 9.16(1) of the FSC's Rule Book requires that a record must be kept of any documents produced when further scrutiny is undertaken of transactions that are complex, large and unusual, or of an unusual pattern of transactions and which have no apparent economic or lawful purpose.

624. For IPA-regulated insurers, IAMLR Regulations 28–30 provide that such records must be kept for at least five years, including for one-off transactions, and kept in such a manner that can be produced and such that the transactions can be reconstructed.

625. Financial institutions informed the assessors that they have developed systems and procedures to identify the categories of transactions and circumstances set out in Recommendation 11. In practice, the systems typically highlight divergences between a customer's actual business and the expected level or nature of activity as set out in the customer's profile, which is required to be maintained by the institution. The divergences are systematically examined by the institution and, if

they cannot be explained, may result in the filing of an STR with the FCU and, potentially in extreme cases, with the termination of the customer relationship.

Special Attention to Countries Not Sufficiently Applying FATF Recommendations (c. 21.1 & 21.1.1):

626. As discussed under Recommendations 5 and 9 in this report, the AML Code 2008 provides for a variety of concessions for financial institutions and other relevant persons from the application of full CDD measures in certain specified circumstances. Pursuant to paragraphs 6(7), 9(7), and 11(6), however, these concessions shall have no effect if the relevant person 'has reason to believe that the country in question does not apply or insufficiently applies the FATF Recommendations'. AML Code 2008 paragraph 8(2)(a)(ii) sets out the requirement for enhanced due diligence where the applicant for business poses a higher risk, which is specified to include a business relationship or one-off transaction with a person or legal arrangement resident or located in a country which the relevant person has reason to believe does not apply or insufficiently applies the FATF Recommendations in respect of the business or transaction in question.

627. For FSC-regulated entities, FSC Rule Book Rule 9.9 on enhanced due diligence includes as part of 'matters which pose a higher risk' a business relationship or one-off transaction with a person or legal arrangement resident or located in a country which the licenseholder has reason to believe does not apply, or insufficiently applies, the FATF Recommendations in respect of the business or transaction in question.

628. For IPA-regulated insurers, IAMLR 2008 Section 6(1) requires insurers to have procedures in place to take into consideration applicants who are located or incorporated in countries on the FATF NCCT list only. While, pursuant to Section 13(2), insurers during the risk assessment process must undertake enhanced CDD for applicants considered high risk, there is no reference in the legislation for insurers to consider if a country does not apply or insufficiently applies FATF recommendations. IGN 2008, which is only applicable for insurers undertaking long-term business, requires insurers to consider the jurisdiction when conducting the risk assessment. IGN2008 Section 1.7 points out that all jurisdictions listed in Schedule 2 of the AML Code 2008 should not be assumed to apply an appropriate standard of AML/CFT regulation and that the list should not be regarded as an automatic trigger to apply reduced CDD.

629. There are no systematic measures in place to ensure that financial institutions are advised of concerns about weaknesses in the AML/CFT systems of other countries. However, relevant information is available to financial institutions from a number of sources with regard to such concerns. FSC licenseholders are required under Rule 9.14(3) to advise the FSC when a foreign branch or subsidiary is unable to apply AML/CFT measures of an appropriate standard. Similarly the IPA requires insurers to submit the same notifications pursuant to Section 3(3) IAMLR 2008. More broadly, the Joint Anti-Money Laundering Advisory Group (JAMLAG) provides a regular forum for public/private sector discussions on AML/CFT issues, which could include concerns about particular jurisdictions. The authorities indicated that they have communicated (directly to licenseholders or via their websites) concerns about specific countries and, for example, warnings issued by the FCU or Customs and Excise.

Examinations of Transactions with no Apparent Economic or Visible Lawful Purpose from Countries Not Sufficiently Applying FATF Recommendations (c. 21.2):

630. Pursuant to AML Code 2008 paragraph 7(3) and in line with Recommendation 21, financial institutions and other relevant persons undertake 'an examination of the background and purpose of the transactions or circumstances' for the categories listed in paragraph 7, which includes transactions that have no apparent economic or visible lawful purpose. Under paragraph 7(4), they must also keep written records of any examination, steps, measures, or determination made or taken and, on request, provide the findings to the competent authorities and auditors. Records required by the Code must be retained for at least five years (paragraph 17(1)).

Ability to Apply Counter Measures with Regard to Countries Not Sufficiently Applying FATF Recommendations (c. 21.3):

631. The authorities did not identify at the time of the assessment any basis on which the IOM could apply appropriate counter-measures to countries that do not apply or insufficiently apply the FATF Recommendations.[42] However, the DHA has the power to remove a jurisdiction from the list in Schedule 2 of the Code of jurisdictions regarded as applying AML/CFT measures equivalent to those of the IOM. The authorities pointed out that, given the size of the jurisdiction, any countermeasures applied by the IOM were unlikely in practice to have significant impact.[43]

3.6.2. Recommendations and Comments

R.21

- The authorities should formalize appropriate means of applying counter-measures to countries that do not or insufficiently apply the FATF Recommendations.

3.6.3. Compliance with Recommendations 11 & 21

	Rating	Summary of factors underlying rating
R.11	**C**	
R.21	**LC**	• The process in place to ensure that financial institutions are advised of concerns about weaknesses in the AML/CFT systems of other countries had not been formalized at the time of the assessment.

[42] This matter was addressed subsequent to the assessment with the coming into force in July 2009 of the Terrorism (Finance) Act 2009.

[43] Subsequent to the assessment, the FSC updated its AML/CFT Handbook to add a new appendix detailing countries where there are concerns about weaknesses in the AML/CFT systems.

3.7. Suspicious Transaction Reports and Other Reporting (R.13-14, 19, 25 & SR.IV)

3.7.1. Description and Analysis

Requirement to Make STRs on ML and TF to FIU (c. 13.1 & IV.1):

632. Pursuant to Sections 17K CJA 1990, 48 DTA 1996 and 11 ATCA 2003 a person may be held criminally liable if he knows or suspect that another person is engaged in laundering the proceeds of a predicate offense, the information or other matter on which that knowledge or suspicion is based came to his attention in the course of his trade, business, profession or employment and the person does not disclose the information or other matter to a constable as soon as is reasonable practicable after it comes to his attention. Additionally, Section 20(2) of the Code requires financial institutions and other relevant persons to establish, maintain, and operate written internal reporting requirements to enable, inter alia, prompt reporting of knowledge or suspicion of money laundering or terrorist financing to the FCU.

633. The Code clarifies that the procedures should relate to disclosure to a constable who is with the FCU. In practice, the inverted nature of the STR reporting requirement 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 financial institutions on whether or not to file an STR with the FIU.

634. The STRs received by the FCU are analyzed in the following comprehensive published statistics.

Financial Crime Statistics

Disclosure Made Under	2004 –05		2005–06		2006–07		2007–08	
Drugs	211	9.11%	86	3.80%	314	19.01%	85	5.45%
Crime	2,059	88.94%	2,168	95.72%	1,329	80.45%	1,468	94.04%
Terrorism	45	1.94%	11	0.49%	9	0.54%	8	0.51%

Type of Business	2004 –05		2005–06		2006–07		2007–08	
Accountant	21	0.91%	18	0.79%	9	0.54%	20	1.25%
Building Society	86	3.71%	71	3.13%	40	2.42%	11	0.70%
CSP	164	7.08%	144	6.36%	153	9.26%	94	6.02%
Financial Advisor	1	0.04%	1	0.04%	1	0.06%	4	0.26%
Investment/Fund Manager	18	0.78%	15	0.66%	17	1.03%	12	0.77%
Lawyer	20	0.86%	15	0.66%	17	1.03%	15	0.96%
Life Assurance/Insurance Company	963	41.60%	803	35.45%	576	34.87%	322	20.63%
Money Service	11	0.48%	6	0.26%	19	1.15%	3	0.19%
Online Gambling	1	0.04%	7	0.31%	5	0.30%	2	0.13%
Other	47	2.03%	23	1.02%	19	1.15%	7	0.45%
Post Office	3	0.13%	2	0.09%	1	0.06%	3	0.19%
Private Bank	133	5.75%	79	3.49%	84	5.08%	95	6.09%
Retail/Offshore Bank	818	35.33%	967	42.69%	677	40.98&	926	59.32%
Stockbroker	1	0.04%	6	0.26%	1	0.06%	1	0.06%
Trust Company	28	1.21%	108	4.77%	33	2.00%	46	2.95%

Financial Crime Statistics

Grounds for Suspicion	2004 –05		2005–06		2006–07		2007–08	
Cash Deposits /Withdrawals	81	3.50%	51	2.25%	69	4.18%	62	3.97%
Cash Purchase/High Value Goods	4	0.17%	2	0.09%	0	0.00%	1	0.06%
Complicated Trust/Corporate Structure	12	0.52%	10	0.44%	16	0.97%	23	1.47%
Evidence of Forged Documentation	11	0.48%	14	0.62%	17	1.03%	9	0.58%
Fiscal	0	0.00%	0	0.00%	255	15.44%	412	26.39%
Foreign Authority Enquiry	14	0.60%	11	0.49%	17	1.03%	12	0.77%
Forex Transactions	6	0.26%	6	0.26%	2	0.12%	1	0.06%
Fraud/False Accounting	498	21.51%	627	27.68%	233	14.10%	377	24.15%
High Risk Jurisdiction	15	0.65%	7	0.31%	15	0.91%	12	0.77%
High Risk Source of Funds	14	0.60%	13	0.57%	17	1.03%	13	0.83%
Investment not consistent with income	38	1.64%	20	0.88%	15	0.91%	10	0.64%
KYC	73	3.15%	53	2.34%	53	3.21%	43	2.76%
Local Police/Regulator Enquiry	24	1.04%	23	1.02%	17	1.03%	19	1.22%
Media/Publicity	40	1.73%	41	1.81%	48	2.91%	43	2.76%
Money Laundering	856	36.98%	818	36.11%	492	29.78%	165	10.57%
Non Clearance of Deposits	0	0.00%	3	0.13%	0	0.00%	1	0.06%
Operation not as expected	346	14.95%	227	10.02%	173	10.47%	189	12.11%
Policy Purchase/Surrender	81	3.50%	63	2.78%	71	4.30%	54	3.46%
Politically Exposed Person	23	0.99%	21	0.93%	28	1.69%	23	1.47%
Public Sector Corruption	18	0.78%	11	0.49%	6	0.36%	6	0.39%
Service of PPP Order	1	0.04%		0.04%	0	0.00%	0	0.00%
Service of Production Order	7	0.30%	9	0.40%	5	0.30%	4	0.26%
Service of Restraint Order	7	0.30%	4	0.18%	5	0.30%	3	0.19%
Transitory Accounts/Immediate Layering	8	0.35%	17	0.75%	4	0.24%	4	0.26%
UK Police/Authority Enquiry	13	0.56%	55	2.43%	21	1.27%	10	0.64%
Unsatisfactory Source of Funds	125	5.40%	158	6.98%	73	4.42%	65	4.16%

Customer Status	2004 –05		2005–06		2006–07		2007–08	
An Existing Customer prior to Dec 1998	1,195	51.62%	780	34.44%	442	26.76%	390	24.98%
A New Customer SINCE 1998	1,120	48.38%	1485	65.56%	1,193	72.22%	889	56.95%
N/A	0	0.00%	0	0.00%	17	1.03%	47	3.01%

Current Business Status	2004 –05		2005–06		2006–07		2007–08	
Continued	1,499	64.75%	1,302	57.48%	932	56.42%	922	59.06%
Closed	645	27.86%	776	34.26%	561	33.96%	278	17.81%
New Business Accepted	29	1.25%	23	1.02%	18	1.09%	14	0.90%
New Business Declined	111	4.79%	130	5.74%	105	6.36%	85	5.45%
Application Pending	31	1.34%	34	1.50%	19	1.15%	24	1.53%
N/A	0	0.00%	0	0.00%	17	1.03%	3	0.19%

Residence of Subject	2004 –05		2005–06		2006–07		2007–08	
Isle of Man	118	5.10%	126	5.56%	105	6.36%	64	4.10%
UK	593	25.62%	842	37.17%	576	34.87%	634	40.61%
EU	291	12.57%	308	13.60%	172	10.41%	148	9.48%
Other	1,313	56.72%	989	43.66%	799	48.37%	480	30.75%
Total	2004 –05		2005–06		2006–07		2007–08	
	2,315		2,265		1,652		1,561	

635. According to the Chief Constable's Annual Report, the reduction in the overall numbers of STRs in 2006 should not be seen as indicating any relaxation in the fight against money laundering. On the contrary, higher levels of awareness within the financial services industry and a better understanding of when to report suspicious activities combined to create more focused and relevant reporting. The higher percentage of reports made in relation to drugs reflects increasing awareness within the industry of the financing of the local drug trade. As mentioned elsewhere in this report, the Constabulary's use of financial investigation to target local drug dealing has got off to a successful start. The number of reports made by professionals, such as advocates and accountants, remains low.

636. The pattern of statistics is consistent with the information obtained by the assessors in all meetings with financial institutions. Levels of knowledge of AML/CFT requirements and awareness of risk and typologies was found to be exceptionally high. Systems, arrangements, and training were in place to facilitate the identification and internal reporting of potential suspicious activities or transactions, and the filing of STRs with the FCU. In terms of the effectiveness of implementation, a possible issue arose from the discussions with financial institutions regarding the length of time between the formation of the initial suspicion and its reporting to the FCU. It appears that it is not unusual for more than one week to elapse while the financial institution makes internal or other enquiries to seek to substantiate the possible suspicious transaction. While it is important that such enquiries are conducted and background material gathered to add value to the STR, efforts should be made to expedite STR reporting in line with the requirement of the AML Code 2008 for prompt reporting.

SR.IV.1

637. Pursuant to Section 14 ATCA 2003, financial institutions and other persons may be held criminally liable if the knowledge or suspicion relates to the terrorism financing offenses within the scope of that Act. Additionally, Section 20(2) of the AML Code 2008 which requires financial institutions and other relevant persons to establish, maintain, and operate written internal reporting requirements to enable, inter alia, prompt reporting of knowledge or suspicion of money laundering or terrorist financing to the FCU.

638. Section 14 ATCA includes within its scope cases where a person knows, suspects, or has reasonable grounds for knowing or suspecting that another person has committed an offense under Sections 7–10 ATCA. These sections cover a range of offenses relating to fund-raising for the purposes of terrorism and the provision, use, and possession of money or other property for the purpose of terrorism. The provisions do not explicitly refer to funds linked or related to terrorist acts, terrorist organizations, or those who finance terrorism but are applied under Section 2 ATCA to organizations proscribed in Schedule 2 to the UK's Terrorism Act 1990.

STRs Related to Terrorism and its Financing (c. 13.2):

639. Section 11 ATCA 2003 makes it an offense for any person to not report any suspicion relating to offenses under the ATCA, including terrorism financing. As with ML, the requirement to file an STR in respect of knowledge or suspicion of FT is set out as the offense of non-reporting of suspicions rather than worded as a direct reporting obligation.

640. In addition, Section 14 ATCA 2003 provides that it is a criminal offense for a person in the regulated sector to not disclose his knowledge or suspicion or his reasonable grounds for suspecting

that another person has committed an offense under Sections 7–10 ATCA 2003 to a constable as soon as practicable. The provision only applies, however, where the information on which the knowledge or suspicion is based came to him in the course of a business in the regulated sector.

641. As outlined in section 2 of this report, the terrorism financing offenses under the ATCA 2003 fall short of the international standard in a few areas. Accordingly, the scope of the reporting requirement involving funds to finance terrorism would also be limited.

642. Financial institutions stated that they would be required to report promptly to the FCU any knowledge or suspicion of FT.

No Reporting Threshold for STRs (c. 13.3):

643. The provisions as outlined above refer to knowledge or suspicion of specific illegal activity relating to ML or FT and are not limited in scope to transactions. There is also no specific reference in the requirements to attempted transactions. All of the financial institutions interviewed during the assessment stated that any suspicious attempted transactions and, more significantly in the context of the IOM, attempts to commence a business relationship would be reported to the FCU. A number of STRs submitted arise from the new business application process, particularly where prospective customers are unwilling to provide the required CDD information, unwilling to identify beneficial owners, or reveal information that would point to criminal activity, including actual or potential tax evasion in the IOM or elsewhere. A number of financial institutions informed the assessors that in such cases they would decline the business and file an STR with the FCU.

Making of ML and TF STRs Regardless of Possible Involvement of Tax Matters (c. 13.4, c. IV.2):

644. The reporting requirements make no reference to tax-related matters and they are therefore not excluded from the scope of the STR reporting offenses of the CJA 1990, the DTA 1996, and ATCA 2003. While there is no offense of tax evasion in the IOM, failure to submit a tax return is an offense and tax evasion could, in principle, be prosecuted as ‘false accounting’ pursuant to Article 19 Theft Act 1982, which is a predicate offense for money laundering. The requirement to report suspicious transactions therefore is considered to apply regardless of whether they are thought, amongst other things, to involve tax matters.

645. In practice, financial institution informed the assessors that they consider they are obliged to report to the FCU all cases of suspicion of tax-related offenses, whether the suspicion relates to the IOM or otherwise. A material spike in the trend of STR reporting statistics in 2005 is attributable in part to information coming to the attention of the financial institutions regarding likely noncompliance with tax requirements in the context of a South African tax amnesty and the EU Savings Tax Directive.

646. The offenses set out in the ATCA refer to knowledge or suspicion of specific illegal activity relating to terrorism and specified financing activities. They are therefore not limited in scope to transactions. There is no specific reference in the requirements to attempted transactions. All of the financial institutions interviewed during the assessment indicated their understanding that in practice attempted transactions could give rise to the filing of an STR.

647. There is no reference to tax-related matters and so they are not excluded from the scope of the STR reporting offenses under the ATCA 2003. This issue is discussed in more detail in the analysis above of R.13.

Additional Element - Reporting of All Criminal Acts (c. 13.5):

648. As outlined in section 2 of this report, IOM law does not require dual criminality; all predicate offenses for money laundering therefore extend to any conduct committed abroad, regardless of whether or not the conduct constitutes an offense in the country where it was committed.

Protection for Making STRs (c. 14.1):

649. Sections 17A(3)(a), 17B(5)(a), 17K(4)(b), and 21 CJA 1990; Sections 46(3)(a), 47(5)(a), (48)(4) and (6) DTA, 1996; and Sections 12 and 15 ATCA provide broadly-worded protection from any liability for breach of a restriction on disclosure of information imposed by statute or otherwise. Any person reporting knowledge or suspicion of criminal activity pursuant to the three acts is therefore protected by law from criminal liability for disclosure of information where required to do so by statute or otherwise.

650. Some of the above provisions are particularly relevant to the business of financial institutions while others apply to any person. While the financial institutions did not raise with the assessors any concerns regarding the scope or degree of protection afforded to them or their staff in the context of reporting suspicions related to ML or FT, the provisions are not sufficiently explicit to comply with the international standard for the following reasons:

- They do not clarify that the protection applies to the financial institution as well as to their directors, officers, and employees (permanent and temporary);
- They do not explicitly provide protection against civil liability or refer to contracts and it would be a matter for judicial determination as to whether the scope of the protection applies;
- There is no limitation that the protection should apply only where the disclosure is made in good faith to the FIU.

651. It is not clear that the protection is available even without identifying precisely the underlying criminal activity or establishing that illegal activity actually occurred.

Prohibition Against Tipping-Off (c. 14.2):

652. The provisions addressing tipping-off specify the circumstances in which a person would commit an offense by tipping off rather than directly prohibiting it. Sections 17D CJA 1990 and 49 DTA 1996 provide that, with regard to tipping-off, a person is guilty of a criminal offense where he knowingly discloses to any person information about:

- an ongoing or proposed investigation by law enforcement;
- a disclosure to the FCU;

- an internal disclosure to the MLRO (e.g., within a financial institution)

relating to ML offenses covered by the Act, comprising 'information or any other matter which is likely to prejudice' an investigation. Schedule 6 to the POCA 2008 came into operation on October 22, 2008 and inserted a new Section 21A into the CJA 1990. The effect of the new section is to create a new 'tipping-off' offense to address a situation in which an institution disclosed that it had been served with a Section 21 order by the AG seeking information relating to an investigation in another institution.

653. Pursuant to Sections 17D(4) and 49(4) DTA 1996, professional legal advisors are excluded from the scope of the provision when giving advice to a client or to any person in contemplation of, in connection with, or for the purposes of legal proceedings. Section 27 ATCA adopts a similar approach and includes a range of similar offenses with regard to FT, but does not directly prohibit tipping-off.

654. The financial institutions did not raise any concerns with the assessors regarding the coverage or nature of the tipping-off provisions. A number of them confirmed that their internal AML/CFT procedures include measures to avoid tipping-off.

Additional Element—Confidentiality of Reporting Staff (c. 14.3):

655. There are no explicit measures in place to ensure that the names and personal details of staff of financial institutions that make an STR are kept confidential. However, the staff of the FCU are covered by the Official Secrets Act and information received by the FCU is covered by the confidentiality provisions of the CJA 1990, the DTA 1996, and the ATCA 2003, in addition to the Data Protection Act 2002. Only authorized personnel have access to STR data in the FCU's database. Financial institutions questioned on this matter during the assessment did not appear to be concerned that their names might be revealed and confirmed that they would expect MLROs and other staff to be prepared to give evidence in open Court as needed. The authorities pointed out that, should it ever be warranted in specific Court cases due to safety or confidentiality concerns, they could apply to the judge for a public-interest indemnity to keep private the names and identities of witnesses.

Consideration of Reporting of Currency Transactions Above a Threshold (c. 19.1):

656. The IOM authorities have considered the feasibility and relative utility of introducing a threshold-based reporting system for currency transactions, most recently on the basis of a paper prepared by the FCU in April 2008. The assessors were provided with a copy of a meeting minute of a working group consisting of the key authorities addressing AML/CFT issues that confirmed that they considered the FCU paper in August 2008 and endorsed the position of the FCU, following consultations with the FSC and DHA, that such a reporting system was not feasible for the IOM. The authorities determined that the continuation of the current system based on suspicious transaction reporting was more appropriate for the IOM.

Additional Element—Computerized Database for Currency Transactions Above a Threshold and Access by Competent Authorities (c. 19.2): Additional Element—Proper Use of Reports of Currency Transactions Above a Threshold (c. 19.3):

657. The authorities opted not to introduce a system for reporting large currency transactions.

Feedback to Financial Institutions with respect to STR and other reporting (c. 25.2):

658. The FCU, by means of the Chief Constable's annual report, publishes very detailed statistics on STRs received, with appropriate breakdowns. The latest published statistics are included in this report in the analysis of Recommendation 13.

659. The FCU also provides feedback on typologies and trends, including through seminars and presentations, some given jointly with the regulatory authorities. Advisory Notices are also produced and circulated to licenseholders on the latest threats, offenders, or trends. Typology information is communicated to the industry through the respective regulatory authorities, regular press releases, and lectures. Case feedback is also given as appropriate.

3.7.2. Recommendations and Comments

R.13

- The FCU and supervisory authorities should take steps to enhance the timeliness of reporting of suspicious transactions to the FCU.
- The law should be amended to provide comprehensively that suspicious attempted transactions must be reported promptly to the FCU.

R.14

- The authorities should amend the law to extend the protection for persons reporting suspicions to the FIU to cover all aspects in the international standard and limit the protection to reporting in good faith.
- The authorities should consider introducing measures to ensure the confidentiality, including in Court proceedings, of persons reporting suspicions to the FIU.

SR.IV

- The authorities should amend the law as needed to address the deficiencies in the scope of ATCA 2003 and thereby provide the required scope of coverage for STR reporting.
- The FCU and supervisory authorities should take steps to enhance the timeliness of reporting of suspicious transactions to the FCU, including for suspicions of FT.
- The law should be amended to provide comprehensively that suspicious attempted transactions must be reported promptly to the FCU.

3.7.3. Compliance with Recommendations 13, 14, 19 and 25 (criteria 25.2), and Special Recommendation IV

	Rating	Summary of factors underlying rating
R.13	**LC**	• Scope to improve timeliness of reporting of STRs to the FCU. • Comprehensive requirement needed to report attempted transactions that raise suspicions.
R.14	**PC**	• The scope of the protection for STR reporting is not sufficient to include all categories of person or circumstances in the international standard and is not limited to good faith reporting.
R.19	**C**	
R.25	**LC**	Section-specific rating would be: C
SR.IV	**PC**	• The scope of the FT reporting requirement is limited by the incomplete coverage of ATCA 2003. • Scope to improve timeliness of reporting of STRs to the FCU. • Comprehensive requirement needed to report attempted transactions that raise suspicions.

Internal controls and other measures

3.8. Internal Controls, Compliance, Audit and Foreign Branches (R.15 & 22)

3.8.1. Description and Analysis

Establish and Maintain Internal Controls to Prevent ML and TF (c. 15.1, 15.1.1 & 15.1.2):

660. AML Code 2008 paragraph 4(1)(a) sets out the requirements for financial institutions and other relevant persons to establish and operate procedures in relation to identification procedures (the term used to encompass the CDD provisions of the Code); record keeping; internal reporting and reporting to a constable (the FCU) of suspicious transactions; staff screening; and AML/CFT preventive procedures in general. Paragraph 4(1)(b) of the Code requires a relevant person to ensure that employees are made aware of these procedures and AML requirements and paragraph 4(1)(c) requires that appropriate training is provided. AML Code paragraphs 6(1), 7(1), 11(1) each requires that a relevant person must establish, maintain, and operate procedures in relation to new business, continuing business relationships, and introduced business, respectively. Paragraph 20(2) of the Code requires a relevant person to establish, maintain, and operate written internal reporting procedures in relation to the reporting of suspicious transactions. Paragraph 21 of the Code requires a relevant person to establish, maintain, and operate procedures in relation to staff screening. These provisions broadly comply with the international standard.

661. AML Code paragraph 4(2) makes it an offense not to comply with paragraph 4(1).

662. In addition, for FSC licenseholders, the FSC Rule Book 2008 provides for risk management and internal control rules. However, these are in parts of the Rule Book in force for existing licenseholders from January 1, 2009 and, being beyond the timeframe of this assessment, are not analyzed further for purposes of this assessment. However, a number of regulatory requirements, in force at the time of the assessment, are relevant, as follows:

(a) For banks, Paragraph 42/87 of the Banking (General Practice) Regulatory Code 2005 provides that a bank shall have adequate policies and procedures relating to AML/CFT. Paragraph 42/87 includes a requirement that the bank shall have a comprehensive operational risk management policy that is appropriate to the nature and scale of its business.

(b) For licenseholders under the Investment Business Act 1991, the equivalent legislation is the Conduct of Business Regulatory Code 2000, Paragraph 6.

(c) CSPs and TSPs are covered by the Fiduciary Services (General Requirements) Code, Paragraph 9(1) which sets out detailed requirements for documented internal controls, systems, and procedures.

663. For IPA-regulated insurers, the requirement for undertaking a risk assessment; implementation of procedures, policies, and controls; record retention and reporting obligations are set out in IAMLR 2008 and further detailed in IGN 2008.

664. IAMLR 2008 includes the following relevant provisions: the CDD requirements including identification and verification of the applicant and beneficial owner (Section 9); the undertaking of a risk assessment process, including the requirements to apply enhanced CCD and disapply simplified CDD in certain circumstances (Section 13); on-going monitoring throughout the business relationship (Section 18); the appointment and responsibilities of the MLRO (Section 26); record keeping at a minimum of five years with a longer period if required by the FCU (Section 29); staff screening and training requirements pursuant to Sections 31 and 32; and the STR reporting procedures including attempted transactions that may be suspicious are set out in Section 27.

665. Financial institutions interviewed during the assessment confirmed that they have developed and documented AML/CFT procedures, addressing all of the required matters. In many cases, these procedures draw also on the experience of the UK and other parents of the financial institutions.

15.1.1

666. AML Code 2008 paragraph 20(1) requires that the financial institutions or other relevant person shall appoint a Money Laundering Reporting Officer (MLRO), that this person must be sufficiently senior within the organization, and must have the right of direct access to the directors, managing board, or partners of the relevant person. The provision does not specify that the MLRO must be at management level as required for compliance with the international standard, but the essential elements of such status are captured by the language of the provision. This role of the MLRO is further specified in Paragraph 20(2) of the Code with regard in particular to the internal management procedures for the identification and reporting of suspicious transactions.

667. For IPA-regulated insurers, IAMLR 2008 Section 26 requires that the board of the insurer shall appoint a Money Laundering Reporting Officer (MLRO), that this person must be able to act independently and must have the right of direct access to the board of the insurer where necessary. The provision contained in Section 26(3) specifies that the MLRO will be treated as a manager for the purposes of Section 29 of the IA 2008.

668. Where the MLRO function may be undertaken by a person who is not an employee of the insurer, such as in the case of an insurance manager, pursuant to IAMLR 2008 Section 4 the MLRO must be of sufficient seniority and experience to undertake the role, and must have direct access to the insurer's board.

669. AML Code 2008 paragraph 20(2)(e) requires financial institutions to have written reporting procedures that ensure that the MLRO has full access to information which may be of assistance to him and which is available to the relevant person. While the qualification 'available to the relevant person' could undermine the effectiveness of the measures, particularly with respect to documentation held on behalf of the relevant person by third parties, including eligible introducers, in or outside the IOM, the AML Code 2008 has strengthened the requirements in relation to access to such information and records, as described earlier.

670. For insurers regulated by the IPA, IAMLR 2008 Section 26(6) specifies that the MLRO must have access to all documents and files, no matter where such records be held, as required to undertake the MLRO role. Such provisions extend to include the MLRO role undertaken by an insurance manager whether or not the access to documents and records is expressed in any agreement or not.

Independent Audit of Internal Controls to Prevent ML and TF (c. 15.2):

671. There is no requirement in law, regulation, or other enforceable means to maintain an adequately resourced and independent audit function (having regard to the size and nature of the business), as would be needed for compliance with the international standard.

672. IPA-regulated insurers are required, pursuant to IAMLR 2008 Section 36 to have in place compliance monitoring procedures to ensure that the MLRO regularly monitors the implementation and operation of the ML and TF procedures and controls. This must include monitoring the effectiveness of techniques employed to raise awareness and training of relevant staff.

673. In practice, as many of financial institutions are part of international groups, they are subject to comprehensive group internal audit processes. The assessors confirmed with many of the financial institutions met, that group internal audit work—and to a significant degree the scope of external audit testing—encompasses ML/FT risk and related AML/CFT internal controls.

Ongoing Employee Training on AML/CFT Matters (c. 15.3):

674. AML Code 2008 paragraph 4(1)(c) provides that a financial institution or other relevant person shall not form a business relationship with or for another person unless the relevant person provides education and training in accordance with the Code's requirements for staff training as set out in Paragraph 22.

675. AML Code 2008 paragraph 22 sets out comprehensive requirements in compliance with the international standard in relation to education and training, as follows. A financial institutions or other relevant person shall provide or cause to be provided education and training including refresher training (not less than annually) for all directors or, as the case may be, partners, all other persons involved in its management, all key staff and appropriate employees to ensure that they are aware of -

(a) the provisions of the money laundering requirements;

(b) their personal obligations under the money laundering requirements;

(c) the internal reporting procedures established under paragraph 20;

(d) the relevant person's policies and procedures to prevent money laundering;

(e) the relevant person's customer identification, record-keeping and other procedures;

(f) the recognition and handling of suspicious transactions;

(g) their personal liability for failure to report information or suspicions in accordance with internal procedures; and

(h) new developments, including information on current techniques, methods and trends in money laundering and the financing of terrorism.

676. The FSC Handbook Section 7 also sets out guidance for licenseholders on providing suitable AML/CFT training.

677. IAMLR 2008, Section 32 contains the provisions in relation to providing appropriate and ongoing ML and TF training for all staff including

(a) Information on new developments;

(b) Current ML and TF techniques including methods and trends;

(c) A clear explanation of the relevant significant aspects of applicable laws and obligations and the requirements concerning suspicious transaction reporting.

678. Additionally, specific training must be in place for senior management, specific AML staff and holders of key control positions. There is no provision relating to the frequency of training contained in IAMLR 2008. However, IGN 2008 Section 11.5.2, applicable only to insurers undertaking long-term insurance, requires that training must be undertaken at least annually.

679. Both IAMLR 2008 and IGN 2008 require that all new employees be given education and training on the avoidance of ML and prevention of FT 'as soon as reasonably practicable'.

680. Financial institutions interviewed during the assessment confirmed that AML/CFT staff training is given a high priority, in the implementation of systems and procedures to comply with the above legal requirements. The training can take a variety of forms, including computer-based,

classroom-style, and in the form of clinics at which particular cases or types of risk situation could be analyzed and resolved. Financial institutions indicated that they maintain detailed records of AML/CFT training received by each relevant staff member and that these records are reviewed in the course of regulatory on-site visits.

Employee Screening Procedures (c. 15.4):

681. AML Code 2008 paragraph 21 requires a financial institution or other relevant person to establish, maintain, and operate appropriate procedures to satisfy itself of the integrity of new directors or partners (as appropriate) and of all new appropriate employees. The Code does not define appropriate employees in this context. For FSC licenseholders, the matter is discussed in detail in the FSC Handbook 2008 Section 7.2 where appropriate employees is explained as not being unique to high-level staff but may include other members of staff (e.g., frontline staff) where there are ML or FT risks. The Handbook sets out a number of screening measures that should be implemented, including obtaining and confirming references, confirming employment history, requesting details of any regulatory action taken against the job applicant, or of any criminal convictions.

682. Pursuant to IAMLR 2008 Section 31, staff screening procedures must be in place, for both the insurer and, where relevant, the insurance manager, for the purposes of confirming integrity and abilities appropriate to the new employee's role.

683. Financial institutions interviewed during the assessment confirmed that they apply strict vetting procedures to all applicants for employment.

Additional Element—Independence of Compliance Officer (c. 15.5):

684. AML Code 2008 paragraph 20(1) requires that the MLRO must have the right of direct access to the directors, managing board, or partners of the financial institution or other relevant person. IAMLR 2008 Section 26(1) also requires that the MLRO must have the right of access to the board of directors where necessary.

Application of AML/CFT Measures to Foreign Branches & Subsidiaries (c. 22.1, 22.1.1 & 22.1.2): Requirement to Inform Home Country Supervisor if Foreign Branches & Subsidiaries are Unable Implement AML/CFT Measures (c. 22.2):

685. With effect from December 18, 2008, AML Code 2008 Paragraph 14 introduced a requirement that financial institutions and other relevant persons ensure that any branch or subsidiary outside the IOM take measures consistent with the Code and guidance issued by a competent authority, to the extent permitted by the laws and regulations of the country in which the subsidiary or branch is located. For FSC licenseholders, FSC Rule Book 2008 Rule 9.14 sets out similar requirements, in line with the international standard. Both AML Code 2008 Paragraph 14 (for all relevant persons) and, for FSC licenseholders, Rule Book Rule 9.14 further provide that they must:

(1) ensure that any branch or subsidiary in a country or territory outside the IOM takes measures consistent with the AML Code 2008, the FSC Rule Book 2008 and AML/CFT guidance, to the extent permitted by the laws and regulations of that country or territory.

(2) where the minimum AML/CFT measures in such a country or territory differ from those required by IOM law, ensure that any branch or subsidiary in that country or territory applies the higher standard, to the extent permitted by the laws and regulations of that country or territory.

(3) inform the IOM competent authority when a branch or subsidiary is unable to take any of the measures referred to in paragraph (1) or (2) above because it is prohibited by the laws and regulations of the country or territory concerned.

686. For IPA-regulated insurers, Section 3 of IAMLR 2008 provides that insurers with branches or subsidiaries in other jurisdictions must apply practices consistent with the IAMLR requirements for equivalent business. In addition, IGN 2008 Section 1.9 sets out the relevant provisions whereby branches or subsidiaries in other jurisdictions must implement procedures consistent with IGN 2008. Where requirements of the host jurisdiction differ, the insurer must comply with IGN 2008. Pursuant to Section 1.9.2, insurers are required to comply with any requirement imposed by the host jurisdiction that is more onerous than those imposed by the IGN 2008. In addition, Section 1.9.3 requires insurers to ensure that the requirements of IGN 2008 are met in particular where the branch or subsidiary is in a jurisdiction that it may have reason to believe does not apply, or insufficiently applies, the FATF recommendations.

687. With the exception of IPA-regulated insurers, there is no requirement in law, regulation, or other enforceable means that financial institutions must pay particular attention that the principles of Recommendation 22 are observed with respect to any branches and/or subsidiaries in countries which it believes does not apply, or insufficiently applies, the FATF Recommendations.

688. In practice, this Recommendation is currently of limited applicability in the IOM as the most typical structure for IOM financial institutions is that they are subsidiaries or (in a few cases) branches of non-IOM financial groups, rather than that themselves operate subsidiaries or branches abroad. To put this in context, at the time of the assessment, the IOM had three banks with overseas branches and a small number of insurance licenseholders abroad whose ultimate parent is an IOM entity.

Additional Element—Consistency of CDD Measures at Group Level (c. 22.3):

689. There is no specific requirement in law, regulation, or other enforceable means to apply consistent CDD measures at the group level, taking into account the activity of the customer with the various branches and majority owned subsidiaries worldwide. However, as noted, this issue has limited applicability in the IOM. For IPA-regulated insurers, IAMLR 2008 and IGN 2008 set out the relevant provisions requiring branches and subsidiaries in other jurisdictions to implement procedures consistent with IAMLR 2008 and IGN 2008.

3.8.2. Recommendations and Comments

R.15

- The authorities should supplement current provisions by introducing in law, regulation, or other enforceable means a requirement that, having regard to the size and nature of the

business, financial institutions maintain an adequately resourced and independent audit function to test compliance with AML/CFT procedures.

3.8.3. Compliance with Recommendations 15 & 22

	Rating	Summary of factors underlying rating
R.15	**LC**	• There is no requirement in law, regulation, or other enforceable means expressly covering AML/CFT to maintain an adequately resourced and independent audit function (having regard to the size and nature of the business).
R.22	**C**	

3.9. Shell Banks (R.18)

3.9.1. Description and Analysis

Prohibition of Establishment Shell Banks (c. 18.1):

690. There is no explicit prohibition[44] on the establishment of a shell bank in the IOM. However, a license issued by the FSC pursuant to FSA 2008 Section 7 is required in order to conduct any activity regulated by that Act, which includes deposit taking. Section 6 provides that a license will not be issued under Section 7 unless the FSC is satisfied that the applicant is managed and controlled in the IOM.

691. The law is supplemented by the FSC's General Licensing Policy, the latest version of which was approved by the FSC Board on July 1, 2008. Paragraphs 3.2.1–3.2.5[45] of the Policy specify that "It is a fundamental requirement that a licenseholder should not be a mere shell and as such a license applicant should establish a 'real presence' in the IOM. An applicant can demonstrate real presence by satisfying the FSC that the business's centre of activity will be in the IOM." If the license applicant is an IOM incorporated company, real presence in the IOM should be demonstrated by the company's management and control being in the IOM. A branch of a company incorporated in another jurisdiction, must demonstrate real presence by registering as a foreign company that has established a place of business in the IOM (under the Companies Act 1931; a 2006 Act company would not be accepted). The centre of regulated business should be in the IOM and there should be a sufficient degree of local management and control to ensure that there is accountability in the IOM for the conduct of the regulated activities. There should normally be two resident officers. All records relating to the business must be located in the IOM or be accessible from the IOM without recourse to

[44] Compliance with Recommendation 18 does not require a legal prohibition against shell banks, though such a provision would represent an effective basis for such compliance. In the absence of a direct legal provision, comprehensive licensing requirements can also provide an effective response to deter the establishment of shell banks.

[45] In a post-assessment revision to the policy, this text (unchanged) was moved to Paragraph 2.8.1.

third parties. (This is subject to any outsourcing, or branch, arrangements for which the FSC might give consent.) While the requirements to maintain records specifies that they be held in the IOM or be accessible within 24 hours, FSC Rule Book Rule 8.26 allows for records to be maintained by third parties, including outside the IOM, in specified circumstances.

692. The FSC's licensing policy allows the operation in the IOM of a 'managed business', though this facility appears to be subject to controls sufficient to preclude the operation of a shell bank.[46] Paragraph 3.3.1[47] of the FSC's General Licensing Policy sets out that although the FSC will not license a business that is a mere shell without real presence in the IOM, it may grant a license to an applicant which on its own does not fully meet the 'real presence' test providing the business of the applicant is to be managed in the IOM by another licenseholder.

Prohibition of Correspondent Banking with Shell Banks (c. 18.2):

693. In the context of correspondent banking services, Rule 9.12(2) of the FSC Rule Book 2008 and AML Code 2008 paragraph 13(2) provide, respectively, that a licenseholder/relevant person must not enter into or continue a relationship with a shell bank.

Requirement to Satisfy Respondent Financial Institutions Prohibit of Use of Accounts by Shell Banks (c. 18.3):

694. Rule 9.12(3) of the FSC Rule Book 2008 and AML Code 2008 paragraph 13(3) provide, respectively, that a licenseholder/relevant person must not enter into or continue a relationship to which this rule applies with a financial institution in a country or territory outside the IOM unless it is satisfied that the respondent bank does not permit its accounts to be used by shell banks.

695. In discussions with financial institutions, the assessors did not encounter any indication that IOM financial institutions provide services to shell banks.

3.9.2. Recommendations and Comments

none

3.9.3. Compliance with Recommendation 18

	Rating	Summary of factors underlying rating
R.18	**C**	

[46] At the time of the assessment, there was one 'managed business' providing banking services that was not managed within the same financial services group. A number of others were managed within financial services groups. Under the FSA 2008, any managed operation must be managed or administered by a licenseholder within a specific financial services license (Class 7) in addition to its own authorization. The managing licenseholder must have the same class of license as the managed operation.

[47] In a post-assessment revision to the policy, this text (unchanged) was moved to Paragraph 2.9.1.

Regulation, supervision, guidance, monitoring and sanctions

3.10. The Supervisory and Oversight System—Competent Authorities and SROs. Role, Functions, Duties, and Powers (Including Sanctions) (R. 23, 29, 17 & 25)

3.10.1. Description and Analysis

Regulation and Supervision of Financial Institutions (c. 23.1):

696. For the most part, IOM financial institutions are subject to adequate AML/CFT regulation and supervision. A small number of areas in which further development is warranted for full compliance with the international standard are noted below.

697. In terms of the legal framework, the AML Code 2008, as secondary legislation, provides for a wide range of measures to comply with many of the relevant FATF Recommendations. In scope, it covers all financial institutions. The 2008 version of the Code is a substantial improvement on the previous AML Code 2007 and moves the IOM much closer to compliance with the detailed provisions of the FATF Recommendations and makes the Code largely consistent with the FSC Rule Book 2008. The few residual deficiencies in the Code have been noted elsewhere in this report.

698. For FSC-regulated entities, the FSC Rule Book 2008, Part 9 deals in detail with AML/CFT and came into effect for all licenseholders on August 1, 2008. The Rule Book, therefore, applies to all licensed banks and all types of investment businesses relevant for purposes of this assessment. It also applies to an important component in the IOM of the DNFBPs (the TSPs and CSPs); this aspect is analyzed in section 4 of this report. While the Rule Book is up-to-date and comprehensive in its coverage, as outlined elsewhere in sections 3 and 4 of this report, some additions are needed to comply fully with the international standard. The Rule Book is supplemented by the substantial guidance contained in the FSC Handbook 2008; while not regarded as enforceable in its own right, many of the provisions of the Handbook use mandatory language and it appears to be the main source of AML/CFT regulatory material used by the financial institutions.

699. For IPA-regulated insurers, the provisions contained in the IA 2008 and the IAMLR 2008 apply. The IAMLR 2008 deals specifically with the prevention and detection of ML and, pursuant to Section 5, covers the countering of financing of terrorism. However, some possibility for confusion and possibly legal arbitrage between the AML Code 2008 and IAMLR 2008 may still exist. IAMLR 2008 only applies to insurers, with other areas of the insurance industry such as insurance intermediaries and managers subject to the provisions of AML Code 2008. IAMLR 2008 is supplemented by IGN 2008, which have been accepted as enforceable for purposes of this assessment; however the guidance notes apply only to insurers undertaking long-term insurance business.

700. Regulation and supervision of money-services business in the IOM was transferred with effect from August 1, 2008, from the registration system previously operated by Customs and Excise to the regulation and supervision of the FSC. However, full application by the FSC of AML/CFT measures for money-services businesses did not come into effect until January 1, 2009 and, as such is beyond the scope of this assessment.

701. The table below confirms that all financial institutions are subject to authorization requirements and supervision. As noted, the structural limitations to the application of AML/CFT measures are as follows :

(a) Supervision by the FSC of money-services businesses was to commence from January 1, 2009;

(b) The IAMLR 2008 imposes requirements on insurers, but excludes from its scope insurance intermediaries and managers, registered scheme administrators, and scheme trustees; and

(c) The IGN applies only to long-term insurers.

Category of financial institution:[48]	**Licensed under:**	**Regulatory Authority:**
Banks / Deposit takers	FSA 2008	FSC
Building Societies/other societies[49]	FSA 2008	FSC
Investment businesses and services to collective investment schemes[50]	FSA 2008	FSC
Money services businesses[51]	FSA 2008	FSC
Insurance business	IA 2008	IPA
Insurance intermediaries	FSA 2008	FSC
General Insurance Business Intermediaries	IA 2008	IPA
Registered Scheme Administrators	Retirement Benefits Schemes Act 2000	IPA
Insurance Managers	IA 2008	IPA
Moneylenders	Moneylenders Act 1991	Office of Fair Trading

[48] Another potential category is credit unions. Although provided for in legislation, none has ever been formed.

[49] There were three building society authorizations in issue at the time of the assessment, all of them relating to the IOM operations of UK building societies.

[50] They conduct business in the IOM under the following categories: stockbrokers, asset managers for collective investment schemes, financial advisers, managers and administrators of collective investment schemes. Their activities, respectively defined as class 2 and 3 in the Regulated Activities Order 2008, correspond to the following in the definition in the FATF methodology: trading in money market instruments, foreign exchange, exchange, interest rate and index instruments, commodity futures trading, participation in securities issues and the provision of financial services related to such issues, individual and collective portfolio management, safekeeping and administration of cash or liquid securities on behalf of other persons and otherwise investing, administrating or managing funds or money on behalf of other persons.

[51] Responsibility for authorizing money services businesses (MSB), including bureaux de change passed to the FSC on the coming into force of the FSA 2008 on August 1, 2008. The MSBs were previously registered by Customs and Excise. The FSC began to apply a supervisory regime (including AML/CFT measures) to the MSBs with effect from January 1, 2009.

Position as at: December 18, 2008	**Institutions covered:**	**Scope includes AML and CFT?**
CJA 1990	All covered entities	AML only
AML Code 2008	All covered entities	AML covered explicitly, CFT by interpretation[52]
FSC Rule Book	All FSC licenseholders (banks, investment business, services to collective investment schemes, CSPs, TSPs, and MSBs)	AML and CFT
FSC Handbook	All FSC licenseholders (banks, investment business, services to collective investment schemes, CSPs, TSPs, and MSBs)	AML and CFT
Insurance Act 2008 (IA 2008)	All insurance businesses	AML and CFT
IPA Insurance Regulations (IAMLR 2008)	Insurers[53]	AML and CFT
IPA Insurance Guidance Notes	Insurers (long-term business)	AML and CFT

702. While the level of effectiveness of implementation of the AML/CFT requirements is difficult to assess in practice, the assessors found across all financial institutions interviewed a high level of awareness of AML/CFT risks, typologies, and international and IOM requirements. It was clear that many of those interviewed had been closely involved in the recent updating and development of the AML/CFT system. Relatively few weaknesses in implementation were identified by the assessors, and those encountered are referenced in section 3 in the analysis of the appropriate FATF Recommendations. Both the authorities and most of the financial institutions were proactive in identifying the main ML and FT vulnerabilities of the business conducted in and from the IOM, namely the dependence on non face-to-face business with nonresidents, often with the business introduced by third parties. The risks and risk mitigants in this area of business are analyzed in the discussion on Recommendations 5, 8, 9 and elsewhere. However, the inherent risks in this area and the extent of use of concessions in the conduct of CDD (including the broad-ranging Acceptable Applicant, Suitable Certifier; fiduciary account; and Introducer and Eligible Introducer arrangements) call into some question the possibility of ever achieving full effectiveness of implementation of the AML/CFT preventive measures.

703. The assessors can only record a snapshot of their findings in terms of assessing effectiveness and it rests with the supervisory authorities to evaluate the implementation of the system on an ongoing basis. The analysis below addresses the extent to which such supervision is currently being

[52] Power to issue secondary legislation to include FT within its scope is considered by the authorities to be covered by the use of the words 'or otherwise' in the enabling provision of the CJA 1990. Parliament raised no objection to the resultant Code 2007 or Code 2008.

[53] Not including insurance intermediaries and managers, registered scheme administrators, and scheme trustees

conducted for financial institutions. By contrast to the level of AML/CFT supervisory attention being given (appropriately) to FSC-regulated TSPs and CSPs, the amount of onsite inspection work in banks and insurers in particular has been limited in recent times. In the case of banks, visits to banks focused on risk and governance arrangements, with at least some coverage of AML/CFT in most cases. The limited resources devoted to AML/CFT-specific onsite work is partly the result of the amount of resources which have been devoted to updating the AML/CFT legal framework, in which both the regulatory authorities and the financial institutions and their representatives have been deeply involved. The regulatory authorities planned to increase the number of AML/CFT-related on-site visits to financial institutions in 2009/10, once the institutions have had an opportunity to fully absorb the latest requirements. The financial institutions interviewed during the assessment indicated that they had, for the most part, already implemented the new measures in advance of the effective date, as the lengthy consultative process has given them time to prepare and the new requirements were typically in line with the measures they were already required to have in place for compliance with group requirements (particularly for UK groups).

Designation of Competent Authority (c. 23.2):

704. The above table indicates that all IOM financial institutions have a designated regulatory authority for AML/CFT purposes. The relevant provisions are as follows:

Financial Supervision Commission (FSC):

705. The objectives and functions of the FSC are set out in section 2 of the Financial Services Act 2008. Section 2(1) The functions of the Commission shall, so far as is reasonably practicable, be exercised:

> (a) in a way that is compatible with the regulatory objectives set out in subsection (2); and
>
> (b) in a way that the Commission considers most appropriate for the purpose of meeting those objectives.
>
> (2) The regulatory objectives are —
>
> (a) securing an appropriate degree of protection for the customers of persons carrying on a regulated activity;
>
> (b) the reduction of financial crime; and
>
> (c) supporting the Island's economy and its development as an international financial centre.

Insurance and Pensions Authority (IPA)

706. The constitution and function of the IPA is set out in section 3 and Schedule 1 to the IA 2008. Under its constitution the IPA has a number of statutory objectives including the making of public documents under the provisions of the various Acts in relation to the detection and prevention of financial crime within the IOM as well as continuously supervising and reviewing the administration

and implementation of those Acts. The IPA has the power to make Regulations and Guidance Notes by virtue of Sections 50 and 51 of the IA 2008 respectively and this includes in relation to AML/CFT matters.

707. The assessors note that the FSC's statutory regulatory objectives include 'supporting the IOM's economy and its development as an international financial centre.' Insofar as the FSC may pursue a developmental role, this has the potential to conflict with the effective application of supervisory measures relevant to AML/CFT. The FSC assured the assessors that the provision is interpreted in FSC policy as referring to measures to protect and enhance the reputation of the IOM as a financial center, for which purposes an effective implementation of AML/CFT measures is essential. The content and tone of the FSC's Annual Reports is consistent with this policy approach as is the level of resources devoted over the last two years in particular to updating the AML/CFT framework.

Fit and Proper Criteria and Prevention of Criminals from Controlling Institutions (c. 23.3 & 23.3.1):

708. Statutory fit and proper tests are applied to all license applicants, owners, controllers, directors, and key managers with respect to IOM financial institutions, to ensure their integrity and propriety, in compliance with the international standard. FSC: Fit and Proper requirements in FSA 2008 Section 6:

(1) A license will not be issued under FSA 2008 Section 7 unless the FSC is satisfied that –

(a) the applicant is a fit and proper person to carry on the regulated activity and provide the services described in that application;

(b) any controller or director of the applicant is a fit and proper person to act as such;

(c) such other persons as appear to the FSC to be key persons are fit and proper persons; and

(d) the applicant is managed and controlled in the Island.

(2) In assessing whether an applicant is a fit and proper person under subsection (1), the FSC will have regard to the information before it as to –

(a) the integrity, competence, financial standing, structure and organization of the applicant;

(b) the integrity, competence and financial standing of –

(i) any controller or director of the applicant;

(ii) key persons in relation to the applicant; and

(c) the description of the business the applicant proposes to carry on.

(3) The FSC may publish guidance setting out the criteria that it will normally apply in assessing whether it is satisfied as required by subsection (1).

709. The FSC has also adopted and issued a General Licensing Policy, updated most recently in July 2008, to set out in detail the licensing requirements for each class of financial services business, including the manner in which the fit and proper test is applied. The Policy document indicates that the fit and proper test is both an initial test at the time of granting a license and a continuing test in relation to the conduct of the regulated activities. The test applies both to the business as a whole and

to the individuals responsible for the management and control (including owners) of the business and key persons.

710. Pursuant to the IA 2008, an applicant for authorization must satisfy the IPA 'that the controller, directors, and chief executive (if any) of the applicant are fit and proper persons.' IA 2008 Section 29 further sets out that no authorized insurer shall appoint a person as director, chief executive, auditor, manager, controller or insurance manager of an authorized insurer unless the IPA is satisfied that any person is fit and proper for the proposed position. The IPA also has the power to direct that a person shall not continue to act in any such capacity in the event that the IPA believes them unfit to hold such a position. Similar measures apply under the Retirement Benefits Schemes Act 2000 (Section 19) in relation to registered schemes administrators and relevant trustees.

711. The IPA advised assessors that on receiving any notifications as outlined above, it conducts appropriate due diligence having regard to the position involved and the individual being proposed. In addition to seeking assurance as to the individual's relevant knowledge and experience pertinent to the proposed role, for example by means of examining previous employment history and seeking references, the IPA seeks to ensure that an appropriate degree of integrity is maintained. In this respect, application forms contain appropriate questions seeking clarification on matters relating to criminal prosecutions, court judgments and any previous dismissals or regulatory actions. In addition, background checks, including by reference to law enforcement, are undertaken in certain circumstances. Other external checks using reputable database sources are undertaken including company registry records, insolvency databases, and commercially available database sources where available. Address checks may also be performed where deemed appropriate.

Application of Prudential Regulations to AML/CFT (c. 23.4):

712. In parallel with this assessment, the IOM financial sector has been the subject of an IMF FSAP Update Assessment, as part of which an update was conducted of the 2002/3 FSAP assessment of the Basel Core Principles, IOSCO, and IAIS Codes. The findings of the update assessment are broadly positive, including for the principles of particular relevance for AML/CFT purposes. No significant deficiencies were identified.

Licensing or Registration of Value Transfer/Exchange Services (c. 23.5): Monitoring and Supervision of Value Transfer/Exchange Services (c. 23.6):

713. Up to July 30, 2008, pursuant to the Anti-Money Laundering (Money Service Businesses) Regulations 2002, Money or Value Transfer (MVT) service providers were obliged to register with the Treasury (Regulation 4) which was also granted a power of entry and inspection on those businesses (Regulation 8). The register was maintained by Custom and Excise. At the time of the assessment, there were 19 MVT businesses registered with IOM Customs, including those providing bureaux de change business.

714. Following a public consultation process, regulatory responsibility for MVT services was assigned to the FSC pursuant to the FSA 2008, as it includes 'any service involving money transmission' (FSA 2008, Section 3(1)f)) within the scope of regulated activities. Consequently MVT service providers are to be subject to all requirements provided in the FSA 2008 and related

secondary legislation, and in particular on AML/CFT issues, those set out in Part 9 of the FSC's Rule Book 2008 and Handbook 2008.

715. MVT services qualify as licensable activities unless they satisfy the conditions set in the Financial Services (Exemptions) Regulations 2008 that create an exemption if the person notifies the FSC that he carries on or intends to carry on this activity with an annual turnover related to this activity of no more than GBP50,000.

716. Such services are classified as a relevant business in the AML Code 2008, Schedule 1, Paragraphs 20 and 22) and therefore are required to comply with all its requirements. Whether or not they benefit from an exemption, the authorities confirmed that they must still comply with the requirements of the Code.

717. Full application by the FSC of AML/CFT measures for money-services businesses was due to come into effect from January 1, 2009. Section 3 of the FSA 2008 and the Regulated Activities Order 2008 specifies the activities which constitute 'regulated activities'. Class 6 relates to Money Transmission Services and covers such financial services as:

1. operation of a bureau de change;
2. transmission of money, or any representation of monetary value, by any means;
3. provision of check cashing services; and
4. issue of electronic money.

Class 6 licenseholders are subject to the AML/CFT requirements of Part 9 of the FSC Rule Book in relation to ML and FT.

718. Even though the extension of the regulatory powers of the FSC to such activities occurred only very recently, MVT service providers met by the assessment team seemed aware of the AML/CFT risks resulting from their activities and already implemented detailed CDD measures that went beyond the current IOM legislative requirements.

719. While the authorities indicated that their choice of threshold was (validly) guided by the FATF Recommendations, the threshold for one-off transactions to be exempted from identification requirements, as determined in the AML Code 2008 (EUR15,000) appears excessive in practice when applied to MVT services. The assessors are not aware of any proposal to apply a lower threshold to MVT businesses, including bureaux de change, to a level more appropriate to the nature and risk of the business in the IOM. However, this assessment is based on the threshold in the international standard, with which the IOM complies.

Licensing and AML/CFT Supervision of other Financial Institutions (c. 23.7):

720. Almost all categories of financial institution in the IOM are regulated by either the FSC or IPA, including all institutions within the scope of the Core Principles. As noted above, money services businesses are in the process of inclusion within the FSC's supervisory scope. Beyond these, the only remaining category is lending and leasing companies which are subject to registration by the Office of Fair Trading (OFT), which also conducts a form of fit and proper test on the controllers of the companies using publicly-available or commercial databases. The OFT does not conduct any off-

site or on-site reviews in relation to AML/CFT as this category of financial business is not considered to be of material risk from a ML or FT perspective. However, as a matter of policy, the OFT confirmed its commitment to supporting the wider AML/CFT program.

721. The assessors were informed that 50 percent of the registered MVT service providers (10 from a total of 19) were visited by Custom and Excise over the last five years, who reported that all the businesses visited were found to be aware of their responsibilities under the AML/CFT regulations, including the training of staff and the procedure for filing STRs. All businesses had CDD procedures in place and reported to be compliant with them; no irregularities were noted. Visits by the FSC in relation to AML/CFT compliance under the FSA 2008 had yet to commence at the time of the on-site visit but were planned.

Guidelines for Financial Institutions (c. 25.1):

722. The FSC has provided extensive guidance to licenseholders (financial institutions and DNFBPs subject to FCU regulation) in its Handbook 2008. Matters covered in detail include all aspects of CDD, AML/CFT internal controls in relation to identifying and reporting of suspicious transactions. The IPA's IGN 2008 (though accepted as binding and therefore other enforceable means for the purposes of this assessment) provides useful guidance on the application in practice of AML/CFT measures for long-term insurance business. Whilst not binding, a number of categories of DNFBPs have been issued with guidance issued on implementing and complying with their AML/CFT requirements. The IOM Law Society; DHA, and FSC have all issued guidance pertaining to the implementation of the AML Code 2007, much of which is also relevant to the AML Code 2008. At the time of the assessment, the GSC had developed draft guidance notes to support the Criminal Justice (Money Laundering–Online Gambling) Code 2008.[54] All are useful documents which, as reported to the assessors by DNFBPs interviewed, have been well received by the relevant parties.

Power for Supervisors to Monitor AML/CFT Requirement (c. 29.1):

723. The analysis of Recommendation 23 confirmed that there are appropriately-empowered supervisory authorities in the IOM with regard to all categories of financial institutions. The FSC supervises banks/deposit takers and investment businesses while the IPA is the supervisory authority for insurance business.

724. With regard to the FSC, the FSA 2008 (as with the Acts which it replaced) provides the full range of supervisory powers as well as enforcement and sanctioning powers as described in this report under Recommendation 17. The FSC Rule Book 2008 Part 9 in relation to AML/CFT sets out additional detailed provisions based on the supervisory powers of the FSA 2008. The FSC's supervisory powers are sufficient to monitor and seek to enforce the requirements of the Rule Book, including those with regard to the application of appropriate AML/CFT measures to foreign branches and subsidiaries of IOM financial institutions, as assessed under Recommendation 22 (FSC Rule Book Rule 9.14).

[54] The guidance notes were issued by the GSC subsequent to the assessment, in April 2009.

725. In respect of the IPA, Section 50 and Schedule 7 of the IA 2008, provide the IPA with the power to make regulations relating to the prevention and detection of money laundering in connection with the carrying on of insurance business. In addition, under Schedule 5 of IA 2008 the IPA has additional powers regarding the obtaining of information or documentation and powers of inspection. Similar powers are conferred under Sections 25 to 28 of the Retirement Benefits Schemes Act 2000.

Authority to conduct AML/CFT Inspections by Supervisors (c. 29.2):

726. The FSC has statutory powers under the FSA 2008 which enable it to gather information, as set out in the following table. The powers may be applied to address any or all of the elements of the international standard.

FSA 2008 Schedule 2	**Power:**
Paragraph 1	**Inspection** A power to inspect books, accounts and documents and investigate transactions during reasonable hours.
Paragraph 2	**Request information** A power to call for information that the Commission may reasonably require for the performance of its functions under this Act. Notwithstanding the title, it can be enforced by a Direction.
Paragraph 3	**Require information** A power to require persons to attend an interview or produce documents in the course of an investigation. It can be exercised upon an application made by the FSC to a Justice of the Peace.
Paragraph 4	**Search warrant** This is a power to enter property and take possession of documents in the course of an investigation. It can be exercised on application made on oath by the FSC to a Deemster (a judge).
Paragraph 5	**External inspector** The FSC may authorize any person to exercise on its behalf all or any of the powers conferred by or under this Schedule (2.1 to 2.4 inclusive).
FSA 2008 Section 23	**Reporting Accountants etc** The FSC may require a licenseholder to provide it with a report by an accountant etc. on any matter relating to the affairs of the licenseholder.

727. In practice, FSC supervision is implemented in accordance with the FSC's published Supervisory Approach (most recently updated in January 2007) which calls for an on-site visit cycle of between one and three years, according to the impact and risk rating of the license holder or group in question. The following table sets out visits conducted in the year March 1, 2007 to February 28, 2008 and planned for March 1, 2008 to February 28, 2009. The plan is in accordance with the published Supervisory Approach and performance against the plan is monitored and reported to the Board of the FSC.

FSC Supervision Team	Annual Business Meeting / Business Meeting[55]*		Supervisory[56] and On-Site Risk Assessment[57]		Focus Visits[58]		Total		Person days 2008/2009
	08/09 Plan	*07/08 Actual*	08/09 Plan	*07/08 Actual*	08/09 Plan	*07/08 Actual*	08/09 Plan	*07/08 Actual*	
Banking	**41**	*28*	**0**	*0*	**21**	*31*	**62**	*59*	317
Fiduciary	**21***	*13*	**30**	*21*	**61**	*66*	**112**	*100*	816
Funds	**24**	*9*	**16**	*7*	**3**	*3*	**43**	*19*	306
Investment Services	**26**	*5*	**31**	*22*	**0**	*1*	**57**	*28*	399
Total	**112***	*55*	**77**	*50*	**85**	*101*	**274**	*206*	1,838

** in addition, the Fiduciaries team is carrying out 46 Business Meetings linked to Focus Visits*

728. The above table includes all areas of the FSC's supervision. In relation to AML/CFT, the FSC informed the assessors that, as an approximate guide, in 2007/08 the supervisory visits and the bulk of the focus visits by the fiduciary team would have featured checks on AML procedures, giving a total in the region of 120–130 onsite visits directly relevant to this assessment. However, the indication in the table that there were no supervisory visits recorded for the banking area that could have included coverage of AML/CFT and none planned for 2008/09 requires clarification. The assessors were informed by the FSC that a full set of thorough AML/CFT inspections of banks was conducted following the last IMF assessment report and that the focus visits shown in the table were 'risk-assessment focus visits', many of which included AML as part of the inspection with a specific focus on how banks were assessing higher-risk business; file sampling of the quality of CDD and testing of arrangements such as for reliance on introducers was undertaken. Focus visits for 2009/10 are to include detailed coverage of AML/CFT matters and sample testing of files and procedures. As the AML/CFT requirements have been in the course of redrafting (including detailed consultation with the financial institutions) over at least the past 18 months and have only recently been finalized, the FSC has taken the view that it would be most effective to allow the banks some time to fully

[55] Business Meetings and Annual Business Meetings involve a meeting with the licenseholder's Board or other senior management to discuss developments in the licenseholder's business and in its management and controls.

[56] Supervisory visits are primarily based around reviewing files and processes across a range of the licenseholder's business, including AML/CFT matters.

[57] An On-Site Risk Assessment is primarily a top-down review of corporate governance in higher-impact licenseholders, supported by sampling in selected areas. These were widely used when the approach was launched, but have been less common in recent years, because license holders have been relatively stable in their structure and the FSC explained that, in these circumstances, it can be more effective to absorb the results of the business meeting before deciding where a focus visit should be targeted.

[58] Focus visits test procedures in a particular aspect of the licenseholder's business, which may be AML/CFT. They involve sample testing of files.

implement the updated requirements before commencing a round of AML/CFT-themed focus visits early in 2009/10 to check compliance.

729. The FSC's off-site supervision includes an Annual Desk-Based Review which considers audited accounts, and information supplied by the licenseholder. The risk assessment of the licenseholder is reviewed at this point and in addition may be updated more frequently to reflect information from visits or complaints. Any concerns regarding AML/CFT compliance can be raised in the context of the annual reviews.

730. In respect of the IPA, Schedule 5 of the IA 2008 provides for powers of inspection and associated powers of entry, in relation to authorized insurers. The same powers of inspection exist with regard to pensions scheme administrators and relevant trustees in Section 26 of the Retirement Benefits Schemes Act 2000. The IPA informed the assessors that they operate a program of rolling on-site inspections which includes reviewing documented policies and procedures, books and records, and extends to sample testing. Each visit is followed up with a comprehensive on-site inspection visit report. However, the assessors understand that while coverage of AML/CFT has been included within the scope of such visits, the number of inspections conducted in recent years has been constrained by the limited resources that have been available to the IPA for significant periods of time due to staffing changes; resource levels are currently higher and additional on-site work, including in relation to AML/CFT, is envisaged.

Power for Supervisors to Compel Production of Records (c. 29.3 & 29.3.1):

731. Both the FSC and IPA have statutory powers to compel production of and obtain access to all records, documents, or information relevant to monitoring AML/CFT compliance of the financial institutions they authorize. The powers are as set out in the above sections. Neither supervisory authority requires a court order to enable them to exercise these powers; however, in the event that the required information is not provided by the financial institution, the supervisory authorities can have recourse to legal process, including seeking a court order. Neither supervisory authority could recall ever needing to take such steps to obtain information from IOM financial institutions.

Powers of Enforcement & Sanction (c. 29.4):

732. Both the FSC and IPA have adequate powers of enforcement and sanction in relation to breaches by financial institutions of AML/CFT requirements, as set out in detail in this report in the analysis of Recommendation 17.

Analysis – R.29

733. While the IOM supervisory authorities have all necessary powers to comply with Recommendation 29, the level of implementation and use of those powers by the FSC in relation to banks and the IPA in relation to insurance business needs to be developed further. Both the FSC and IPA indicated that they are in the course of implementing additional on-site programs to test AML/CFT compliance with AML/CFT requirements. In the view of the assessors, for effective implementation of Recommendation 29, additional on-site inspections of banks and insurance businesses are warranted.

734. In recent years, the FSC has conducted frequent and detailed on-site work with particular focus on AML/CFT and including file sampling. This work is taken into account in this assessment in the analysis under Recommendation 12. The FSC explained to the assessors that their prioritization of fiduciaries in this manner reflects their view in the recent past of the need for additional work to be conducted on a risk-sensitive basis to improve the quality of AML/CFT implementation in some of the fiduciaries.

Availability of Effective, Proportionate & Dissuasive Sanctions (c. 17.1): Designation of Authority to Impose Sanctions (c. 17.2):

735. Criminal and administrative sanctions are available for noncompliance with AML/CFT requirements. AML Code 2008, paragraph 4(2) provides that it is a criminal offense to contravene its general requirements. Pursuant to the paragraph 4(2), any person who contravenes the obligation to establish, maintain, and operate AML/CFT procedures (including identification and verification, record keeping, and internal staff screening), is liable to custody for a period not exceeding six months or to a fine not exceeding GBP5000, or to both, on summary conviction; and to custody not exceeding two years or to a fine, or to both, on information.

736. Criminal prosecutions for breaches of the requirements of the Code would be the responsibility of the AG. The authorities confirmed that no referrals were made to the AG in 2007 or 2008 (on the basis that they did not encounter any incidents of breaches serious enough to warrant referral to the AG) and no such prosecutions have been brought.

737. With regard to administrative sanctions, the FSC has available to it a range of possible administrative sanctions which it can apply against a licenseholder which contravenes statutory provisions. Some may lead to an administrative sanction, after having undertaken an ‘action for a breach’ of the Rule Book (FSA 2008, section 19(1)) which refers to the exercise of a wide range of powers that may lead to directions or conditions on licenses, revocation or suspension of a license, and civil penalties, where these fall within the scope of regulations issued by the FSC. Specifically, pursuant to FSA 2008, Section 48(3), an action for a breach may extend to the following :

(a) the revocation or suspension of a license;
(b) the issue of a direction as to fitness or propriety under FSA 2008 Section 10;
(c) the service of a warning notice under Section 11;
(d) the issue of a public statement under Section 13:
(e) the issue of a direction under Section 14;
(f) the imposition of a penalty under Section 16;
(g) an application for an injunction or for restitution under Section 20;
(h) the appointment of a receiver under Section 21;
(i) the appointment of a business manager under Section 22;
(j) the withdrawal of an exemption in accordance with regulations;
(k) the exercise of powers in relation to a permitted person under Schedule 2.

738. The FSC may also use its power of direction (FSA 2008, Section 14), or of restriction of the nature of the licenseholder’s business (Section 8), issue a public statement (Section 13), an injunction (Section 20), appoint a receiver (Section 21) or a manager (Section 22) or decide to suspend or revoke

the licenseholder's license (Section 9). Some of these sanctions are exercisable by the High Court on the application of the FSC.

739. In organizational terms, the FSC divides the work of dealing with noncompliance of its licenseholders between its Supervision Division (administrative matters) and the Enforcement Division (legal sanction). Typically, the Supervision Division would initially identify the breach from information obtained from licenseholders in the course of its on-site and off-site supervision. The first level of response is a visit report, which 'outlines the areas covered and any action required of the licenseholder'. The FSC could choose to immediately initiate a disciplinary action but informed the assessors that it generally engages with the management of the licenseholder to seek to resolve the issue. However, if those approaches are not successful in having the situation regularized, the Supervision Division will initiate an action that may lead to a disciplinary decision by the FSC (e.g., placing a condition on a license, suspension or revocation of the license) and, in parallel, the Enforcement Division may examine the fitness and propriety of the licenseholder's directors or key persons, which could result in the issuing by the FSC of a 'not fit and proper' direction.

740. The FSC may impose on the licenseholder a restriction on the nature of the business it may undertake, either in a public manner (by imposing a condition on a license) or privately (by issuing a direction). The figures concerning those restrictions are as follows:

	Banks	**Fiduciaries**	**Funds and investment services**
Licenses with conditions attached	11	21	11
Licenses with directions attached	21	5	10

Source: FSC, September 16, 2008

741. Some sanctioning powers, such as the appointment by the FSC of a manager to a licenseholder, are too recent for their effectiveness to be assessed; similarly, the effectiveness cannot yet be assessed of activities the supervision of which was recently transferred to the FSC, such as money transmission services for which the licensing process had not yet been completed. Concerning the powers actually used by the FSC to date, there seems to be few sanctions for minor breaches—between June 2007 and June 2008, 202 breach letters were issued by the FSC but few disciplinary actions resulted. For the more serious breaches, the FSC had used its power to revoke a license once prior to the assessment and on a further occasion shortly after the onsite visit. In reality, failing institutions usually opt to surrender their license. The FSC has also taken successful action since 1999 against 36 individual company officers such that they were disqualified under Section 26 of the Companies Act 1992.

742. The FSC sanctioning procedure may take a long time: for example, there was almost a two year period between the first on-site visit of a corporate services provider (CSP) at which issues were identified and raised and the direction being attached to the license. For any breach, but particularly concerning AML/CFT issues, this appears excessively long and is related to the priority given by the Supervision Division to seeking to have the breach regularized in preference to resorting more

quickly to sanctions. The FSC pointed out that this was an extreme example and other cases were concluded more rapidly.

743. On the application of the FSC, the High Court may take decisions that complete the disciplinary actions: as mentioned, pursuant to FSA 2008 Section 20, the High Court can grant an injunction making an order requiring that a person takes such steps as the court may direct to remedy a contravention. It may also impose economic sanctions (Sections 20(2) to 20(5)); pursuant to section 22 of the FSA 2008, the FSC may also prepare an order which would be the grounds for the High Court to appoint a business manager.[59] These new sanctions granted to the judicial power of the IOM are too recent for their effectiveness to be assessed.

744. For IPA-regulated entities, the penalties for offenses are set out in the IA 2008 and are applicable to offenses committed under the Act as well as to offenses committed under any regulations made thereunder. The offenses include breaches in respect of AML/CFT matters. Any breach of the IAMLR 2008 or IGN 2008 renders an insurer liable to regulatory action by the IPA and IA 2008 provides the IPA with the power to apply a range of proportionate and deterrent disciplinary sanctions. As noted elsewhere in the report, IAMLR 2008 applies only to insurers and IGN 2008 only to insurers undertaking long term business.

745. The IA 2008 provides the authority with the power to withdraw authorization (Section 10) or to impose conditions or restrictions; direct that an individual shall not continue to act in the capacity of a director, chief executive, auditor, manager, controller, or insurance manager without the written consent of the IPA (Section 29(3)); require an insurer to take such action as appears necessary to ensure a reduction in the extent to which it is possible for an insurance business to be used for a purpose connected with financial crime (Section 33(1)); apply to the High Court for an injunction in the event there are grounds to believe that any person will contravene any provision of any Regulation made under the Act.

746. Section 37 of IA 2008 provides the IPA with the power to impose civil penalties of such an amount as the IPA considers appropriate. Such civil penalties will be assessed with due regard to the significance of the breach, whether of legislation, regulations, or guidance, and the circumstances surrounding such breach. Civil penalties may be imposed by the IPA against the authorized insurer and/or against designated officers of the insurance business involved.

747. In so far as registered schemes administrators and relevant trustees are concerned, the IPA has the power to direct that any director, chief executive, manager or controller shall not continue to act in that capacity without written consent of the IPA (Section 19 of the Retirement Benefits Schemes Act 2000). The IPA may revoke the recognized status of any scheme if it considers that the trustee or administrator has contravened any provision of the IA 2008 (Section 22(1)).

[59] The Order was made in January 2009 and is the Financial Services (Appointment of Manager) Order 2008 made under the FSA 2008. It was approved by Tynwald on January 20, 2009 and came into operation on January 22, 2009.

Ability to Sanction Directors & Senior Management of Financial Institutions (c. 17.3):

748. Pursuant to AML Code 2008 paragraph 4, criminal sanctions may, among other categories, be applied to directors and senior management of financial institutions, as the provision refers to the 'officers' of a legal person.

749. The FSC may issue 'not fit and proper directions' with the effect of preventing a person against whom the direction is made from being appointed or continuing to exercise their role as a controller, director, or 'key person' (defined in the FSA 2008 Section 48 as individuals with significant powers or responsibilities in a licenseholder), where the FSC 'on reasonable grounds' considers that the individual is not fit and proper (FSA 2008, Section 10). Pursuant to Section 26 of the Companies Act 1992, the FSC may also seek the disqualification of persons, if they are considered as unfit to be director or secretary of a company, liquidator, receiver, or manager of a company's property, or in any way 'whether directly or indirectly, to be concerned or take part in the promotion, formation or management of a company'. This disqualification has a wider effect than the previous action as it applies to the direction of any company, whether licensed or not. The process begins with a 'letter before action' sent to the concerned person. Afterwards, if it is presumed that this person continues to operate in the IOM while the FSC considers him or her as not fit and proper, it is then the High Court's competence to issue a disqualification order that operates for a period between three and 15 years (Section 27). Those two categories of actions enable the FSC to have an effective means, either on its own or at its application, to prevent persons it considers as not fit and proper from conducting a business, whether regulated or not, in the IOM. The IPA indicated that it can and does put persons forward to the FSC for action in respect of Section 26 of the Companies Act 1992.[60]

750. For IPA-regulated entities, Section 37(2) of the IA 2008 allows the IPA to impose a civil penalty, should he consider it appropriate, on a controller, director, chief executive, or senior manager of the institution concerned. This may be in addition to a civil penalty applied to the institution itself.

Range of Sanctions—Scope and Proportionality (c. 17.4):

751. The range of sanctions at the FSC's and IPA's disposal is broad (as listed above) and is completed by the criminalization of AML/CFT breaches pursuant to the AML Code 2008. Moreover, when serious breaches are identified, the action on the licenseholder would usually be accompanied by 'fit and proper' directions.

752. A limitation to the proportionality of the administrative sanctions system as applicable to penalties applied by the FSC is that, under FSA 2008, the extent to which the power may be exercised is dependent on regulations made by the FSC. So far, the FSC only issued a regulation that allows it to impose penalties for late returns[61]. In the absence of further FSC regulations, the scope for the issue of administrative penalties remains overly narrow which, when combined with the low number of

[60] Legislation concerning directors' disqualification was consolidated post-assessment into the Company Officers (Disqualification) Act 2009 which came into effect on June 19, 2009.

[61] Financial Services (Civil Penalties) Regulations 2008.

administrative actions taken and the absence of criminal action to date for breaches of AML/CFT requirements, materially reduces the range of sanctions available in practice to the FSC.

Resources – applying R.30

30.1

753. The FSC is an independent statutory board established under the Financial Supervision Commission Order 1983 which set out its initial remit. This was revised by the FSA 2008 with effect on August 1, 2008. As a statutory board the Commission operates under the Statutory Boards Act 1987 as amended. The FSC Board Members ("Commissioners") are appointed by the Treasury, subject to the approval of Tynwald, the Island's parliament. The legislation prohibits members of Tynwald, civil servants, and employees of a government department or a statutory board (with the exception of the Chief Executive of the FSC) from becoming a Commissioner. At present there are seven Board Members, including the Chairman and the Chief Executive of the FSC.

754. As noted elsewhere in this report, the statutory objectives of the FSC include 'supporting the IOM's economy and its development as an international financial centre.' Insofar as the FSC may pursue a developmental role, this has the potential to conflict with the effective application of supervisory measures relevant to AML/CFT. The FSC assured the assessors that the provision is interpreted in FSC policy as referring to measures to protect and enhance the reputation of the IOM as a financial center, for which purposes an effective implementation of AML/CFT measures is essential. The content and tone of the FSC's Annual Reports is consistent with this policy approach as is the level of resources devoted over the last two years in particular to updating the AML/CFT framework.

755. The FSC is funded from the general revenue of the IOM Government. Costs are offset by license fees paid by institutions and the revenue generated from Companies Registry. There was a surplus of GBP8.7 million in the financial year 2007/08. An annual budget is prepared by the FSC within the budget parameters determined by the IOM Government, which considers requests for increases in funding alongside those received from other Government departments and allocates resources in line with the wider strategic priorities of the Council of Ministers and available revenue.

756. The IPA includes within its mission statement to 'ensure a flourishing environment for IOM business'. However, this is presented in the context of a statement of objectives which include 'without compromising regulatory impartiality, to safeguard the IPA's and the IOM's image'. The IPA Board is required by legislation to include individuals with relevant expertise and experience. The IPA is funded from the general revenue of the IOM, with that cost offset partly by fees collected from licensed institutions. It prepares its budget each year for discussion and agreement with the Treasury and Council of Ministers.

30.2

757. The FSC employs its own staff directly on such terms and conditions as it deems appropriate. The official headcount is 66.5 plus two 'contract staff' giving a total of 68.5. The FSC is structured into five divisions comprising of Supervision, Enforcement & Authorizations, Policy and Legal, Companies Registry and Operations. The Supervision Division of the FSC has an allocation of 29.5

full time equivalent staff. It is responsible for on-site and off-site supervision of licenseholders and most of the powers to intervene in the affairs of a licenseholder.

758. The FSC policy is to hire professional staff of high integrity. In its recruitment, it seeks to balance industry experience with professional qualifications. Police checks for criminal convictions are undertaken on all FSC staff where possible and references are obtained from previous employers and professional bodies. Upon appointment, all officers are required to sign the Official Secrets Act 1989. All information received and discussed by officers is confidential and may not be communicated to third parties either while in office or following resignation, pursuant to the provisions of the FSA 2008.

759. FSC staff are not permitted to hold shares and related investments in FSC-regulated entities. The FSC has a Code of Conduct on Conflicts of Interest, reviewed annually, which aims to reflect the high standards of integrity expected of professionals, to ensure that information is properly handled and to ensure regulatory decisions are not improperly influenced by conflicts of interest.

760. The IPA may appoint such staff on such terms as it considers appropriate to carry out its functions. It currently has a full-time staff of 12 people (including its chief executive). Detailed recruitment practice ensures that its staff has the requisite skills and is of high integrity. All regulatory staff have previous experience of working in relevant areas of the insurance and pensions sector and many also have a relevant professional qualification. All staff are required to sign a declaration under the Official Secrets Act upon commencement of employment. It is an offense under the IA 2008 to disclose any information to third parties except in specified circumstances. Recruitment procedures also include the carrying out of appropriate police checks.

761. In assessing the adequacy of resources, the assessors noted in the analysis of the effectiveness of implementation of Recommendation 29 that there are two areas of particular AML/CFT significance for which the authorities plan additional on-site supervision in 2009/10, namely the FSC-regulated banks and the IPA-regulated insurance businesses. In meetings with a range of financial institutions, the assessors did not identify deficiencies in implementation of AML/CFT requirements that would point to a need for urgent on-site inspections. Nonetheless, given the inherent risk in the financial services business conducted (non face-to-face for non-residents, often based on introduced business and, to some extent, reliance on third parties to conduct CDD), a robust on-site inspection program is warranted. As noted, the FSC is to conduct a further round of AML/CFT focus visits for banks in 2009/10 once the banks have had some opportunity to implement fully the latest revision to the requirements. Also, the IPA plans to increase on-site checking. In both cases, there appears to the assessors to be a need for some increase in supervisory resources.

30.3

762. All new FSC staff receive training from the MLRO regarding their obligations on reporting suspicious activity/transactions upon commencement of their employment, with annual updates. Regular AML/CFT training events are provided in-house by the FSC's Head of Enforcement and his staff to reflect any changes in international standards, IOM law, guidance notes, or in the general approach to preventive measures. Recent training took place on June 23, 2008 (total attendees 38), with further sessions provided by the FSC's MLRO to all FSC staff on STR reporting responsibilities on July 16, August 6, and October 20, 2008. Four sessions had also been conducted in 2007 (August

13, September 21, September 28 and October 5 (total attendees 51). The FSC has introduced a customized e-testing facility operated by KPMG for all supervision staff. This provides both refresher training and identifies any weaknesses in staff knowledge and experience. Any gaps identified are addressed through specific one-to-one training or on a group basis as required.

763. The IPA's staff includes individuals who have held senior positions within the compliance departments of insurance companies and other financial institutions, including acting as MLRO. Such staff spend considerable time dealing with AML-related matters, including participating in relevant courses and seminars and also monitoring developments through relevant publications.

764. In addition, the IPA and the FSC are members of the IOM's Joint Anti-Money Laundering Advisory Group (JAMLAG), part of the purpose of which is to provide a forum for dissemination and exchange of information on AML/CFT matters between the public and private sector. The Chief Executives of the IPA and FSC (in addition to the Chief Executive of the DHA) are the co-chairs of JAMLAG.

765. The assessors were satisfied with the high levels of awareness of AML/CFT issues among supervisory staff and the related training programs of the FSC and IPA.

Statistics – applying R.32

32.1

766. Since at least 2002, the IOM authorities have placed increasing emphasis on the implementation of effective AML/CFT measures. In the 18–24 months prior to this assessment, substantial resources have been devoted to bringing the IOM system into line with the FATF Recommendations 2003, including by reference to the EU Third AML/CFT Directive and developments in the UK and other Crown Dependencies.

767. As described in this report, structures were established to review the systems and their effectiveness, in a spirit of cooperation and consultation between authorities and with the private sector. These structures include the official AML/CFT committee of authorities chaired by the Chief Secretary and the joint committee at which industry participates, JAMLAG. In the context, therefore, of the complete overhaul of the legislative and supervisory framework for AML/CFT over the past two years in particular, the assessors are satisfied that the authorities are reviewing on an ongoing basis the effectiveness of the AML/CFT measures. Once the new provisions have been bedded in, it will be important to continue to conduct a reassessment of effectiveness of the measures on an ongoing basis.

32.2

768. The supervisory authorities maintain reasonably complete statistics on supervisory measures, including on-site inspections that included some coverage of AML/CFT. There is a need for some further refinement of some of the statistics to provide more precise information on the extent to which on-site examinations include AML/CFT work and in relation to the application of some of the administrative sanctions by the FSC.

769. The FSC maintains detailed records and statistics on its requests to and responses to requests from other supervisory authorities, particularly with regard to the IOSCO Multilateral MOU.

3.10.2. Recommendations and Comments

R.17

- The FSC should consider issuing further regulations to allow it to impose additional administrative sanctions, where warranted.

R.23

- The authorities should apply AML and CFT requirements directly to any category of financial institutions not currently covered, having regard to such underlying ML and FT risks as may arise.

- The authorities should consider reducing significantly the current EUR15,000 threshold for the application of CDD measures to one-off transactions by MVT service providers.

- The FSC should proceed as planned to implement a supervisory regime for money-services businesses, including bureaux de change, as soon as possible.

R.29

- The FSC and IPA should make more frequent and extensive use of their powers to conduct AML/CFT on-site inspections of banks and insurance businesses, respectively.

R.30

- Consideration should be given to assigning some additional resources to AML/CFT supervision of banks and insurance businesses, particularly to allow for an increase in on-site inspections.

3.10.3. Compliance with Recommendations 17, 23, 25 & 29

	Rating	Summary of factors underlying rating
R.17	**LC**	• Limitation in the current scope of available administrative sanctions. • The effectiveness of the sanctions system is reduced by the low incidence of disciplinary measures applied by the FSC and the absence of any criminal prosecutions against persons contravening the AML/CFT requirements.
R.23	**LC**	• Coverage of the AML/CFT requirements for financial institutions, though broad, is not fully comprehensive. • There is not yet in place an effective system of monitoring and ensuring

		compliance with AML/CFT requirements for money and value transfer service providers.
R.25	**LC**	Section-specific rating would be: C
R.29	**LC**	• The supervisory authorities should, as planned, avail of their powers to conduct additional on-site inspections of banks and insurance businesses.

3.11. Money or Value Transfer Services (SR.VI)

3.11.1. Description and Analysis (summary)

Legal Framework:

770. Up to July 30, 2008, pursuant to the Anti-Money Laundering (Money Service Businesses) Regulations 2002, Money or Value Transfer (MVT) service providers were obliged to register with the Treasury (Regulation 4) which was also granted a power of entry and inspection on those businesses (Regulation 8). The register was maintained by Custom and Excise. At the time of the assessment, there were19 MVT businesses registered with IOM Customs, including those providing bureaux de change business as assessed under Recommendation 23.

771. Following a public consultation process, regulatory responsibility for MVT services was assigned to the FSC pursuant to the FSA 2008, as it includes 'any service involving money transmission' (FSA 2008, Section 3(2)f)) within the scope of regulated activities. Consequently MVT service providers are to be subject to all requirements provided in the FSA 2008 and related secondary legislation, and in particular on AML/CFT issues, those set out in Part 9 of the FSC's Rule Book 2008 and Handbook 2008.

772. MVT services qualify as licensable activities unless they satisfy the conditions set in the Financial Services (Exemptions) Regulations 2008 that create an exemption if the person notifies the FSC that he carries on or intends to carry on this activity with an annual turnover related to this activity of no more than GBP50,000.

773. Such services are defined as a relevant business in the AML Code 2008, Schedule 1, Paragraphs 20 and 22) and therefore are required to comply with all its requirements. Whether or not they benefit from an exemption, the authorities confirmed that they must still comply with the requirements of the Code.

774. Even though the extension of the regulatory powers of the FSC to such activities occurred only recently, MVT service providers met by the assessment team seemed aware of the AML/CFT risks resulting from their activities and already implemented detailed CDD measures that went beyond the current IOM legislative requirements.

Designation of Registration or Licensing Authority (c. VI.1):

775. Pursuant to the FSA 2008, MVT services moved from a registration to a licensing regime whereby they have been placed under the supervision of the FSC. The licensing process commenced for new applicants from August 1, 2008, but existing companies had until November 1, 2008 to submit an application. FSC supervision was scheduled to commence on January 1, 2009 and any existing MSB wishing to take advantage of the GBP50,000 turnover exemption (and therefore not requiring a license) had to notify the FSC of their activities by January 1, 2009.

Application of FATF Recommendations (applying R.4-11, 13-15 & 21-23, & SRI-IX)(c. VI.2):

776. The remarks concerning the strengths and weaknesses of the IOM secondary legislation on CDD, and particularly the AML Code 2008 apply also to MVT services. The threshold for one-off transactions to be exempted from identification requirements, as determined in the AML Code 2008 (EUR15,000), while validly based on the threshold set for occasional transactions in the FATF Recommendations, appears excessive in practice for MVT services in the IOM. The assessors are not aware of any proposal to apply a lower threshold to MVT businesses to a level more appropriate to the nature and risk of the business.

Monitoring of Value Transfer Service Operators (c. VI.3):

777. The assessors were informed that 50 percent of the registered MVT service providers were visited by Custom and Excise over the last five years. As discussed earlier, no compliance issues were noted.

List of Agents (c. VI.4):

778. A list of agents of MVT service providers were declared in the past to Custom and Excise and will in future be made available to the FSC.

Sanctions (applying c. 17.1-17.4 in R.17)(c. VI.5):

779. The criminal offenses stipulated in AML Code 2008 paragraph 4(2) are relevant as they apply to persons who contravene the AML/CFT requirements of the Code, and to their officers. Regulation 13 of the Anti-Money Laundering (Money Services Businesses) Regulation 2002 allows the Treasury to impose a civil penalty not exceeding GBP5,000 when a business fails to register, or to supply supplementary information, or to comply with Regulation 8 (concerning entry and inspection for customs officers). However, such sanctions are not directly related to CDD. As from August 1, 2008, MVT service providers are subject, as any other FSC licenseholder, to the full range of sanctioning powers under the FSA 2008.

Additional Element—Applying Best Practices Paper for SR VI (c. VI.6):

780. Since the introduction of registration as described above, the IOM authorities did not identify any providers of informal money transmission services operating in or from the IOM. They point to the manner in which the pre-August 2009 registration requirement was introduced in 2002 as evidence that appropriate action was taken to ensure that any informal activities were regularized. However, there would be merit in implementing a program of awareness raising and occasional

testing to ensure as far as feasible that the authorities would become aware of the operation of any informal systems.

3.11.2. Recommendations and Comments

- The FSC should proceed at an early date to conduct AML/CFT supervision of MVT service providers.
- The authorities should implement ongoing measures to identify any informal MVT service providers in the IOM.
- The authorities should consider reducing significantly the current EUR15,000 threshold for the application of CDD measures to one-off transactions by MVT service providers.

3.11.3. Compliance with Special Recommendation VI

	Rating	Summary of factors underlying rating
SR.VI	**LC**	• Active supervision for AML/CFT purposes of MVT providers had not commenced at the time of the assessment.

4. PREVENTIVE MEASURES—DESIGNATED NON-FINANCIAL BUSINESSES AND PROFESSIONS

4.1. Customer Due Diligence and Record-keeping (R.12)

4.1.1. Description and Analysis

781. CDD obligations for DNFBPs are largely the same as those for financial institutions and are subject to the same strengths and weaknesses identified in Sections 3.1 and 3.3 above. Of particular note is the potential risk arising from cross-border non face-to-face business and the challenge of identification of ultimate beneficial owners and controllers, particularly where reliance is placed on third parties to undertake CDD (see Sections 1.6.c and 3.1 above). Trust Service Providers (TSPs) and Corporate Service Providers (CSPs) conduct a great deal of cross-border and non face-to-face business and should, therefore, be considered particularly vulnerable. The on-line gaming sector's entire business is subject to inherent weaknesses in relation to CDD as all business is conducted on a non face-to-face basis, with identification and verification via electronic means.

TSPs and CSPs

782. The TSP and CSP sector forms an integral part of the financial services industry of the IOM. It comprises legal professionals and accountants providing TCSP services; all company formation agents; trust service providers who are not legal professionals; business address and business service providers; and all professional interim managers. The authorities advised that there are approximately 22,000 trusts and 42,000 companies managed or administered in or from the IOM by TSPs and CSPs, respectively.

783. Pursuant to the FSA 2008 Section 3 and the Regulated Activities Order 2008, TSP and CSP activities constitute 'regulated activities'. TSPs and CSPs are authorized and supervised by the FSC.

784. TSPs and CSPs are subject to the AML Code 2008[62] when undertaking activities listed in Schedule 1 of the Code. The list of corporate services or trust services in Schedule 1(16) includes those within the meaning of Section 3 of the FSA 2008 and Classes 4 and 5 of Schedule 1 to the Regulated Activities Order 2008. TSPs and CSPs are also subject to Part 9 of the AML/CFT requirements of the FSC's Rule Book 2008 and to the guidance set out in the FSC AML/CFT Hand Book 2008.

785. Almost all TSPs are either CSPs in their own right or are part of a group which also contains a CSP license holder. The industry in the IOM includes a variety of TSP and CSP corporate structures. A significant number of accounting and law firms have established associate companies that have obtained TSP and/or CSP licenses from the FSC, pursuant to the FSA 2008.

Legal services

786. The legal profession in the IOM consists of advocates and registered legal practitioners. Pursuant to the Advocates Act 1995, persons licensed to practice law are referred to as 'advocates'. In

[62] Which superseded the AML Code 2007 on December 18, 2008.

addition, persons licensed in a number of prescribed jurisdictions may register with the IOM Chief Registrar pursuant to the Legal Practitioners Registration Act 1986 and are known as legal practitioners. Upon registration, legal practitioners are allowed to provide any legal services in the IOM other than those excluded under the Advocates Act 1976, namely court appearances and real estate and probate matters. They may therefore deal with all non-contentious trust, corporate and commercial matters, including conducting financial transactions for their clients relating to the managing of assets, of bank, saving and securities accounts, and the organization of contributions for the creation, operation, or management of companies.

787. Both advocates and legal practitioners are subject to the obligations set forth in the AML Code 2008 when undertaking activities listed in Schedule 1 of the Code. However, only the former are under the ambit of the IOM Law Society. The latter are not subject to any supervision with respect to compliance with IOM law, a matter which the authorities indicated they are in the course of addressing.

788. The list of relevant business activities in Schedule 1 includes (1) the holding or managing of any client assets and (2) the provision of legal services involving the participation in or the planning or execution of a financial or real property transaction for or on behalf of a client and involving the sale or purchase of land; the managing of bank, savings or security accounts; the organizing of contributions for the promotion, formation, operation, or management of bodies corporate; the sale or purchase of business entities; and the creation, operation, or management of a legal structure or legal arrangement.

789. The assessors were advised that the larger law firms in the IOM have associate companies incorporated that are licenseholders regulated by the FSC. All trust and company service related business is conducted through these associated companies and is therefore regulated and supervised by the FSC.

Accountants

790. The IOM accounting profession is subject to the provisions of the AML Code 2008 pursuant to Schedule 1 Section 6 (d) 'An accountant or a person who, in the course of business, provides accounting services'. Accountants, currently numbering 89, are registered by the DHA. Similar to the legal profession, accountancy practices undertaking trust or company services typically establish associated companies that obtain licenses from the FSC pursuant to the FSA 2008.

Casinos

791. The IOM has authorized one terrestrial casino and 11 on-line casinos, offering a variety of gambling options including sports book betting, peer-to-peer betting, poker and other card related on-line games. The casinos are licensed and supervised by the Gambling Supervision Commission (GSC) pursuant to the Casino Act 1986 and Online Gambling Regulation Act 2001.

792. The terrestrial casino is a 'relevant business' under the AML Code 2008 Schedule 1(9) which covers 'any activity permitted to be carried on by a license holder under a casino license granted under the Casino Act 1986'. As such, the casino is required to comply with the same standard as any other regulated business activity.

793. The on-line casinos, which consist of entities that offer on-line gaming such as poker and other card related games, are bound by the provisions of the Online Gambling (Registration and Accounts) Regulations 2008 (OGR 2008) which provides for account opening procedures including identification of the player or business participant, in addition to setting controls on the customer's account deposits and withdrawals. Item 10 of the OGR 2008 Schedule applies the requirements of Section 17F of the CJA 1990 to all online gambling business. Further, licenses issued for online gambling businesses pursuant to Schedule 2 Online Gambling Regulation Act 2001 mandate that the licensee must comply with any AML provisions that apply to the type of gambling permitted under the license. The current provisions relate to the Criminal Justice (Money Laundering) Online Gambling Code 2008 (OG Code 2008), effective September 1, 2008, which replaced the Anti-Money Laundering (Online Gambling and peer to peer gambling) Code 2006. The OG Code 2008 is considered secondary legislation, as detailed in Section 3, due to the powers conferred on the DHA to issue such codes pursuant to CJA 1990 Section 17F. The OG Code's definition of ML and FT details directly the DTA 1996; CJA 1990; and ATCA 2003. However, as discussed in section 3, there is doubt that the DHA is empowered to issue secondary legislation in relation to FT matters.

Real Estate and Dealers in precious stones and metals

794. Real Estate Agents and Dealers in precious stones and precious metals are also subject to the provisions of the AML Code 2008 Schedule 1 (4) and (24), respectively. Item (24) of the Schedule extends the scope of coverage to include 'the business of dealing in goods of any description (including dealing as an auctioneer) whenever a transaction involves accepting a total cash payment of EUR15,000 or more'. Responsibility for licensing and supervision is assigned to the DHA. The assessors met with one high-value goods dealer (a jeweler), who reported the business had never engaged in a cash transaction over EUR15,000.

General coverage of DNFBPs – analysis

795. Overall, the DNFBPs interviewed by the assessors seemed to be well informed about their obligations with respect to CDD and record keeping requirements under the AML Code 2007, which set out the requirements in force at the time of the on-site visit, and the Criminal Justice (Money Laundering) Online Gambling Code 2008, respectively.

796. While some advocates stated that the beneficial owner would be identified in all cases, others indicated that they would try their best to obtain beneficial ownership information but would not always succeed. All parties the assessors interviewed stated that they would not in all cases obtain the required customer due diligence information at the outset of a business relationship or before conducting a transaction but would allow for a grace period for the client to provide the necessary information. It was mentioned by a number of advocates that, in some cases, that would lead to situations in which the matter or transaction for which an advocate was hired was concluded before the grace period was over and client information would not be obtained at all. In such situations, all practitioners indicated that they would not necessarily file an STR with the FCU.

797. In relation to business introduced by third parties, which is the vast majority of new business for advocates, accountants, CSPs, and TSPs, some conduct their own customer due diligence whereas others rely on the customer information provided, under the Eligible Introducer regime, by a foreign counterpart who referred the client.

798. The terrestrial casino, which is part of a hotel complex, applies identification and verification procedures for any person wishing to avail themselves of the gambling-related goods or services offered on the premises. Every person entering the gaming and casino areas must provide original valid government-issued documentation which includes a photograph and signature. This information is validated and recorded electronically which then permits membership to be granted and only members may access the casino premises. The designated thresholds for a single transaction (or in several transactions that appear to be linked) is applied at a threshold lower than the statutory level of GBP2,000/EUR2,500 and as set out in terrestrial casino's operating procedures.

799. The on-line casinos are required to identify the prospective customer before an account is opened and before any transactions are undertaken and further to seek satisfactory evidence of the identity of the participant for designated thresholds of a single transaction exceeding EUR3,000 or where the aggregate of transactions over 30 days amounts to EUR3,000. As demonstrated to the assessors, in order to satisfy themselves with regard to identity, the on-line casinos obtain documentation by electronic means such as scanned copies of identification documentation. Based on this documentation, further checks are undertaken to verify identity using data available electronically including, for example, electoral rolls.

800. All DNFBPs interviewed by the assessors advised that, in compliance with the AML Code 2007 (in force at the time of the on-site visit), records were kept for five years or longer from the day of the termination of a business relationship. On-line casinos maintain records for six years from the last transaction or termination of the business relationship pursuant to Section 13 of OG Code 2008.

CDD Measures for DNFBPs in Set Circumstances (Applying c. 5.1-5.18 in R. 5 to DNFBP) (c. 12.1):

5.1

801. All categories of DNFBPs, excluding on-line casinos, fall under the definition of 'relevant business' in AML Code 2008 Schedule 1. Thus they are required to adhere to all aspects of the Code relevant to this recommendation. The Code does not explicitly prohibit anonymous accounts but paragraph 5(2) requires from all persons conducting an activity in the financial sector that they undertake identification and verification procedures on all applicants for business.

802. The OG Code 2008 applies to on-line casinos and gaming and is secondary legislation made under the powers conferred on the DHA by Section 17 of the CJA 1990 as detailed above. CDD obligations pursuant to OG Code 2008 (4) are explicit that no anonymous accounts or accounts in fictitious names may be maintained.

5.2

803. The requirement to undertake CDD measures is set out in secondary legislation. Pursuant to AML Code 2008 paragraph 6, identification procedures apply to new business relationships detailed in this report under Recommendation 5. In summary, the Code stipulates that relevant persons (which includes DNFBPs other than on-line casinos) must identify the applicant for business before the business relationship is entered into or during the formation of this relationship 'but in any event as soon as reasonably practicable (taking into account the need not to interrupt the normal conduct of

business where there is little risk of money laundering or terrorist financing occurring) after contact is first made' (Paragraph 6(2)).

804. Pursuant to the OG Code 2008 (3)(1), the license holder must establish, maintain, and operate identification procedures requiring a prospective participant to provide satisfactory information as to their identity, subject to the designated threshold of a single transaction exceeding EUR3,000 or where the aggregate of transactions over 30 days amounts to EUR3,000 (7(3)).

5.3

805. The concerns expressed in Section 3.2 on the limitations on verification when CDD is conducted by introducers have equal merit for TSPs and CSPs, although most TSPs and CSPs interviewed reported that they obtain customer identification information from clients or introducers in line with the obligations under the AML Code 2008. On-line casinos are required, pursuant to Section 7 of the OG Code 2008, to verify the customer's identity using reliable, independent source documents when the threshold of one payment or the aggregate over 30 days of EUR3,000 is reached.

5.4

806. The AML Code 2008 paragraphs 5(2) and (3) include requirements to verify that a person purporting to act on behalf of a customer is so authorized, and to identify and verify the identity of that person. The OG Code 2008 requires, pursuant to (8), on-line casinos to establish the legal nature and status of the business participant; identify the ultimate beneficial owner (i); verify that any person purporting to act on behalf of the participant is authorized to do so (iii) and to take reasonable steps to obtain satisfactory evidence to identity and verify the authorized person and the ultimate beneficial owner (iv) and (v).

5.5

807. DNFBPs, like financial institutions, are required under AML Code 2008 paragraphs 6(1) and (3) to establish, maintain, and operate procedures that require:

(a) the identification of the applicant for business:

(b) the verification of the identity of the applicant for business using reliable, independent source documents, data, or information;

(c) the obtaining of information on the purpose and intended nature of the business relationship;

(d) the taking of reasonable steps to establish the source of funds.

These provisions represent a significant clarification and enhancement of the measures that had been required under the AML Code 2007, which was in effect at the time of the on-site visit.

808. A number of advocates advised the assessors that in practice, the work commissioned may have already been completed before verification documentation is received; hence no verification of the beneficial owner was undertaken. The mission was advised that this process occurred under a

risk-based approach where the advocate considered that there was little risk of money laundering or terrorism financing and to proceed otherwise would have interrupted the normal conduct of business.

809. Whereas, pursuant to OG Code 2008 (7.3), the on-line casinos apply the verification thresholds of a single transaction exceeding EUR3,000 and the OG Code (8 (ii)) is explicit in determining the beneficial owner though they only need to undertake 'reasonable steps', pursuant to (8(v)) to obtain 'satisfactory evidence to identity and verify the beneficial owner'.

5.6

810. Paragraph 6(3)(c) of the AML Code 2008 and Section 5 OG Code 2008 impose requirements to obtain information on the purpose and intended nature of the business relationship and all DNFBPs interviewed informed the assessors that they maintained a business profile for each customer.

5.7

811. Pursuant to paragraph 15 of the AML Code 2008, detailed procedures for the ongoing monitoring of the business relationship and similar provisions must be in place. Ongoing monitoring of the business relationship for on-line casinos, pursuant to the OG Code 2008 (10), must be undertaken regardless of the activation of the threshold amount. Additionally for on-line casinos, OG Code 2008 (5) specifies the requirement for risk profiling and ongoing monitoring for variation of pattern of transactions All DNFBPs interviewed informed assessors that they monitored ongoing business relationships. In addition, CSPs and TSPs advised that they monitored all transactions on financial institution accounts of entities for which they provided directorship services.

5.8

812. With effect from December 18, 2008, the AML Code 2008 required relevant persons to carry out a risk assessment in accordance with Paragraph 3 to estimate the risk of money laundering and terrorist financing, having regard to the nature, scale, and complexity of activities; the products and services offered; the customer base; and the extent of reliance on third parties. The assessment is required to be undertaken as soon as possible after the coming into force of the provision. A parallel requirement was brought into force for CSPs and TSPs under the FSC's Rule Book 2008 with effect from August 1, 2008. However, as the requirement was newly-introduced at the time of the on-site visit, it was not feasible for the assessors to form a view on the effectiveness of the measures in place. Early indications from the FSC pointed to a need for additional risk analysis on the part of at least some regulated entities. The analysis in section 3 of this report under Recommendation 5 applies to DNFBPs subject to the AML Code 2008. For online casinos, pursuant to OG Code 2008 (5), the licenseholder must undertake a risk assessment of the potential or existing customer including enhanced due diligence. Such requirements are detailed in the OG Code 2008 (9) and include a natural or legal person or arrangement that is directly or has substantial connection with a PEP; jurisdictions that insufficiently apply FATF recommendations; or the subject of any notices or warnings from the GSC.

5.9

813. Pursuant to paragraph 6 of the AML Code 2008, firms may undertake CDD as soon as reasonably practical taking into the need not to inhibit the normal conduct of business where there is

little or no risk of money laundering. A number of advocates interviewed advised assessors they apply this provision on a regular basis. For on-line casinos, pursuant to OG Code 2008 (6) CDD must be undertaken 'as soon as reasonably practicable' after contact is first made by the potential customer.

5.10

814. For DNFBPs, excluding on-line casinos, consistent with specified requirements and issued guidance, the concessions discussed under Recommendation 5 and those arising under the Eligible Introducer arrangements, are restricted to countries listed in Schedule 2 of the AML Code 2008. If the licenseholder or other relevant person has any reason to believe that the jurisdiction in question does not apply, or insufficiently applies, the FATF Recommendations in respect of the business of that person, the concessions cannot be applied regardless of the inclusion or otherwise in Schedule 2 (AML Code 2008 paragraph 11(6)). For on-line casinos, pursuant to OG Code 2008 (5)(2b), the CDD risk assessment process must consider including the value of funds deposited with the licenseholder; jurisdiction or location of the customer and source of funds and no concessions are granted in relation to identification. The concession in relation to evidence of identity is applicable only to the qualifying payout threshold payments of, or the aggregate over 30 days of, EUR3,000. Regardless of the threshold for qualifying payouts, pursuant to (9)(2) if the licenseholder has any reason to believe that the jurisdiction in question does not apply, or insufficiently applies, the FATF Recommendations in respect of the business of that person, then enhanced due diligence needs to be undertaken regardless of the threshold for qualifying payouts.

5.11

815. DNFBPs subject to AML Code 2008 cannot apply the concessions listed under Recommendation 5 of this report where there is any knowledge or suspicion of ML, pursuant to paragraph 11(11). The Code makes no reference to disapplying the concessions where specific high-risk scenarios apply. The OG Code 2008 does not reference directly the treatment of the qualifying threshold where there is any knowledge or suspicion of ML nor in the risk assessment process.

5.12

816. The review of Recommendation 5 is applicable to DNFBPs subject to the AML Code 2008. For on-line casinos, pursuant to Section 5 of OG Code 2008, a risk sensitive basis is to be applied and guidance is contained in the Online Gambling Guidance Notes for the Prevention of Money Laundering and Countering of Terrorist Financing, which were in the process of being finalized at the time of the assessment.[63]

5.13

817. Like financial institutions, DNFBPs subject to the AML Code 2008 and pursuant to paragraph 6(2) in relation to new business relationships, identification and verification of identity must take place before a business relationship is entered into, or during the formation of that

[63] The Guidance Notes were published subsequent to the assessment, in April 2009.

relationship, but in any event it must take place as soon as reasonably practicable (taking into account the need not to interrupt the normal conduct of business where there is little risk of money laundering or terrorist financing occurring) after contact is first made between the relevant person and the applicant for business. The criticism in section 3 of this report relating to the degree of discretion allowed regarding to the timing of identification and verification is also valid for DNFBPs. The assessors were advised by TSPs and CSPs interviewed that no new entity was formed for a new client before completing the CDD requirements. On-line casinos, pursuant to OG Code 2008 Paragraph 6(1) must obtain satisfactory information to identify the customer as soon as reasonably practical after contact is first made between the license holder and the customer. If such information is not evident or satisfactory pursuant to (6)(2), the license holder cannot open a customer account, accept money, or permit any participation in online gambling.

5.14

818. Paragraph 6 of the AML Code 2008 provides DNFBPs, like financial institutions, a conditional option of delaying collection of CDD information and documents in the event of a low risk transaction where otherwise it may interrupt the normal course of business as detailed in the analysis in section 3 of Recommendation 5. In relation to on-line casinos, if such customer identification information is not evident or satisfactory pursuant to OG Code 2008 (6)(2), the license holder cannot open a customer account' accept money' or permit any participation in online gambling.

5.15

819. The AML Code 2008 has introduced a requirement (in paragraphs 6(9) and 7(6) that a relevant person, including DNFBPs, should consider filing an STR where it is unable to comply with fundamental CDD requirements, whether for an existing or prospective customer. There is no equivalent measure for casinos contained in the OG Code 2008. A number of advocates interviewed advised assessors that failure to complete the CDD when the work engagement had already been completed did not immediately raise dialogue with the FCU; however, any instances where suspicions arose were brought to the attention of the FCU.

5.16

820. In the context of continuing business relationships, AML Code 2008 paragraph 7(6) requires that the business relationship shall not proceed any further in the event that satisfactory CDD information and verification documentation (referred to in the Code as evidence of identity) is not obtained or produced, the relevant person shall consider terminating the relationship, and consider whether an STR should be filed. Interviews with DNFBPs elicited reports of business declined and existing relationships terminated resulting from existing clients' refusal to provide customer and beneficial owner information as required by the relevant Codes.

5.17

821. DNFBPs subject to AML Code 2008 are required to apply CDD requirements to existing business relationships, including upon the occurrence of defined 'triggers' relating to perceived

changes in circumstances. This includes where anything arises to cause doubt as to the adequacy of CDD information and documentation already held pursuant to paragraph 7(2).

822. The OG Code 2008 is explicit in the requirements for on-line casinos to have procedures in place for ongoing and effective monitoring of any transactions and pursuant to paragraph (10), includes reviewing information in relation to the customer's identity and verification information. Trigger events such as transactions significantly different in number or value to the normal pattern of previous transactions require confirmation of information of identity and verification of identity pursuant to (10)(3). Where such satisfactory information is not provided in relation to identification and verification, no further participation in online gambling by the customer is permitted.

5.18

823. No cases of anonymous accounts were identified to the assessors. Should such a case ever arise, AML Code 2008 paragraph 7 requires that, where a financial institution or other relevant person becomes aware that the CDD information or documentation held is inadequate, they must take steps to obtain adequate information or documentation. OG Code 2008 is explicit that no anonymous accounts are permissible pursuant to Paragraph 4 (1a).

CDD Measures for DNFBPs in Set Circumstances (Applying Criteria under R. 6 & 8-11 to DNFBP) (c.12.2):

6.1

824. The AML Code 2008 introduced a detailed definition of a politically-exposed person (PEP), a set of requirements in Paragraph 10 for senior management-approved acceptance procedures for PEPs, and a requirement under paragraph 8 for the application of enhanced CDD measures to customers identified as PEPs. These measures represent a significant strengthening of the requirements compared with those in place at the time of the onsite visit, although, in the case of CSPs and TSPs, Rule 9.11 of the FSC Rule Book (being applicable to CSPs and TSPs) already required PEPs to be treated as a higher risk.

825. While not binding, guidance notes have also been issued detailing the identification and recommended treatment of PEPs. CSPs and TSPs are subject to the FSC Handbook 2008 which contains relevant guidance. The IOM Law Society, of which all advocates are members, issued guidance detailing identification, verification, and recommended treatment for PEPs. The DHA has issued guidance on ML and FT for DNFBPs which addresses PEPs and other high risk situations in sections 5.9 and 5.10 respectively.

826. For the online gaming industry, OG Code 2008 paragraph 2 contains a detailed definition of a PEP and sets obligations under (9) for enhanced due diligence, including PEPs.

827. All advocates, legal practitioners, accountants, CSPs and TSPs, and online and terrestrial casinos interviewed advised assessors that they used commercially available database services and internet search engines to check PEP status and applied a higher due diligence.

6.2

828. With effect from December 18,2008, the AML Code 2008 introduced a mandatory requirement for senior management approval for a range of actions in relation to PEPs. In addition, for FSC-regulated CSPs and TSPs, FSC Rule Book Rule 9.11(2) requires licenseholders to maintain appropriate procedures and controls for requiring the approval of its senior management, before establishing a business relationship or continuing an existing business relationship with a PEP.

829. While the OG Code 2008 requires the identification of PEPs and the subsequent treatment of such customers as a higher risk, senior management approval is not mandated.

830. All DNFBPs interviewed advised the assessors that they required senior management approval following their own internal procedures, for establishing business relationships with any PEP.

6.3

831. There is no explicit requirement for most DNFBPs to take reasonable measures to establish the source of funds of PEPs, although the AML Code 2008 has introduced a relevant requirement under paragraph 6(3) to take reasonable steps to establish the source of funds for all new business relationships, which would include any PEPs. Additionally, paragraph 8(3)(c) of the AML Code 2008 requires the taking of reasonable measures to establish the source of wealth of the customer and any beneficial owner in the context of enhanced CDD conducted on PEPs. Moreover, FSC Rule Book Rule 9.7, which applies to licensed CSPs and TSPs, requires reasonable steps be taken to establish the source of funds for all customers, which would include any PEPs. FSC Rule Book Rule 9.9, in applying a requirement for enhanced due diligence measures to PEPs stipulates that licenseholders must take reasonable measures to establish the source of the wealth of the customer and of any beneficial owner when a PEP is involved in a business relationship.

832. OG Code 2008 (9) (1) requires licenseholders to apply enhanced due diligence to customers posing a higher risk, including PEPs. Such enhanced due diligence for PEPs, pursuant to (9) (3) includes taking reasonable measures to establish the source of any funds and of the wealth of the customer and the beneficial owner and the underlying principal.

6.4

833. Enhanced ongoing monitoring of PEP accounts falls within the obligations to monitor ongoing business relationships in the relevant Codes. The assessors were advised during interviews that in practice, all DNFBPs that reported having PEP clients indicated that senior management was involved in ongoing transaction monitoring of such clients.

8.1

834. Effective December 18, 2008, the AML Code 2008 introduced in paragraph 23 a requirement that a relevant person maintain appropriate procedures and controls to address the risk of abuse of new technologies for ML or FT purposes. For FSC-regulated CSPs and TSPs , FSC Rule Book Rule 9.13 requires that licenseholders maintain appropriate procedures and controls to prevent the misuse of technological developments for ML or FT purposes. However, the authorities have not built on these broad requirements to guide the relevant persons on the range of issues that they would expect to see addressed in the procedures.

8.2

835. Non face-to-face business is prevalent for CSPs, TSPs, lawyers and accounting businesses and is inherent for on-line casinos. While there are no provisions in primary legislation, the AML Code 2008 has introduced requirements (in paragraphs 5(5), 6(6), 7(5), 9(5), and 15(3) that adequate measures must be taken by relevant persons to compensate for any risk arising as a result of dealing with an applicant for business, on ongoing relationship, or a one-off transaction (respectively) other than on a face-to-face basis.

836. For FSC-regulated CSPs and TSPs, pursuant to FSC Rule Book Rules 9.6(4) and 9.15(3), licenseholders must take adequate measures to compensate for any risk as a result of not dealing face-to-face with the customer. Although not binding, this topic is addressed also in the guidance set forth by the DHA and the IOM Law Society. Other than the requirements to identify the beneficial owner contained in the OG Code and, for TSPs and CSPs only, the identification of the beneficial owner and the treatment of introduced business set forth in the FSC Rulebook, there are no additional requirements concerning the conduct of non-face to face relationships.

9

837. As with financial institutions, many customers of TSPs, CSPs, lawyers, and accountants are introduced by a third party. AML Code 2008 paragraph 11 sets out the basis on which CDD measures should be applied where business is introduced by a third party. It also defines the class of introducer commonly known as an ‘eligible introducer’ and sets out the eligibility criteria to permit reliance on them by DNFBPs subject to the Code. The provisions are analyzed in detail under Recommendation 9 in section 3 of this report and apply equally to DNFBPs subject to the AML Code 2008. The recommendations and analysis presented in Section 3.2 are equally valid here.

10

838. Like financial institutions, DNFBPs must keep records for five years as prescribed in the AML Code 2008 paragraph 17 and, in the case of on-line casinos, six years pursuant to the OG Code 2008. DNFBPs interviewed by assessors confirmed that such requirements are implemented at a minimum.

11

839. DNFBPs subject to the AML Code 2008 are required, pursuant to paragraph 15, to establish, maintain, and operate procedures to monitor ongoing business relationships as detailed in Section 3.2.

The OG Code 2008 is explicit as to the requirements for on-line casinos to have procedures in place for ongoing and effective monitoring of any transactions and, as described above, includes review of information in relation to the customer's identity and verification information both on the occurrence of trigger events and in the normal course of business.

4.1.2. Recommendations and Comments

- The authorities should keep under review the list of categories of higher-risk customers and consider including additional categories on a risk-related basis.

- The authorities should conduct a risk-based review of the current scope of the Acceptable Applicant facility and, if warranted, limit its availability for consistency with the FATF Recommendations.

- In the case of CSPs and TSPs, if the exceptions to the CDD requirements of secondary legislation as currently set out in the FSC Handbook are to be retained, the authorities should amend the secondary legislation as necessary to provide for them.

- The authorities should review on a risk basis the implementation of the concession allowing operations to commence prior to completion of full CDD procedures to ensure it is not being misused, particularly in the case of advocates.

- The DHA should proceed as quickly as possible with the planned arrangements to ensure that effective AML/CFT arrangements are place for accountancy professionals, including on a risk-sensitive basis those that are not members of either of the two main bodies.

- The DHA should proceed as soon as possible with the planned implementation on a risk-sensitive basis of AML/CFT measures for dealers in high-value goods engaged in cash transactions.

- The requirement to consider filing an STR if unable to adequately complete CDD measures should be extended to casinos.

4.1.3. Compliance with Recommendation 12

	Rating	Summary of factors relevant to s.4.1 underlying overall rating
R.12	**PC**	• Implementation arrangements for AML/CFT requirements were not yet in place for the accountancy profession. • In the case of CSPs and TSPs, the exceptions to the CDD requirements currently in the FSC Handbook lack a firm legal basis. • Effectiveness of implementation of the supplemental provisions of the AML Code 2008, other than for CSPs and TSPs, could not be assessed as they were adopted subsequent to the on-site visit.

4.2. Suspicious Transaction Reporting (R.16)

4.2.1. Description and Analysis

Introduction:

840. All DNFBPs are subject to the STR reporting requirements under the CJA 1990, ATCA 2003, and DTA 1996, as outlined under section 3 of this report. DNFBPs (other than on-line casinos) are also subject to the provisions of Section 20 of the AML Code 2008, while on-line casinos are subject to Section 16 of the OG Code 2008 with regard to STR reporting.

841. CSPs and TSPs fall within the supervisory mandate of the FSC and are subject to the provisions of the FSA 2008, the FSC Rule Book 2008 and the additional guidance set out in the FSC Handbook 2008, as detailed in section 3.

842. In relation to the legal profession, Section 17K of CJA 1990 allows for an exemption from the reporting requirement for 'legal advisers' in privileged circumstances, whereby any information or matter is considered privileged if it is communicated or given by a client or his representative in connection with the giving of legal advice or by a person seeking legal advice or by any person in contemplation of or in connection with and for the purpose of legal proceedings. It is expressly stated that information communicated or given to the legal adviser to further any criminal purpose may not be considered privileged. The IOM Law Society advised assessors that, in cooperation with counsel, it has just concluded the drafting of legislation that would allow for onsite audits of law firms for AML/CFT purposes while respecting the rules pertaining to legal privilege. The practitioners interviewed by assessors stated that they would determine the application of the legal privilege based on the transaction or matter in question and not based on the client. Therefore, if a certain matter relating to one specific client is privileged but a different matter of the same client is not, the privilege would attach only to the first matter and would not prevent the filing of an STR for the second.

843. Within the casino sector, both on-line and terrestrial, assessors were advised by the entities interviewed that they were aware of the obligations placed upon them pursuant to CJA 1990 Section 17F , Section 16 of OG Code 2008, and Section 20 of the AML Code 2008 in relation to the recognition and reporting of suspicious transactions.

844. All DNFBPs interviewed advised assessors that they had appointed a designated MLRO at senior management level to receive, review and, if applicable, forward STRs to the FCU directly. All advised awareness of their obligations in relation to STRs. While the MLROs do not analyze STRs, they do review the report to substantiate that there are grounds for suspicion.

845. A detailed statistical analysis of STRs submitted to the FCU can be found in the discussion of Recommendation 13 of this report. The following data have been extracted for DNFBPs and indicate relatively low levels of STR reporting by the legal and accountancy professions and by on-line gambling businesses. Only the CSPs have sustained a significant level of reporting.

Type of Business	2004 –05		2005–06		2006–07		2007–08	
Accountant	21	0.91%	18	0.79%	9	0.54%	20	1.25%
Lawyer	20	0.86%	15	0.66%	17	1.03%	15	0.96%
TSP	28	1.21%	108	4.77%	33	2.00%	46	2.95%
CSP[64]	164	7.08%	144	6.36%	153	9.26%	94	6.03%
Online Gambling	1	0.04%	7	0.31%	5	0.30%	47	3.01%
Other	47	2.03%	23	1.02%	19	1.15%	7	0.45%

Requirement to Make STRs on ML and TF to FIU (applying c. 13.1 & IV.1 to DNFBPs):

846. All DNFBPs, like financial institutions, are required by law to file STRs when a suspicion arises. In relation to secondary legislation, DNFBPs other than online casinos, are bound by the provisions of the AML Code 2008 detailed in Section 3. On-line casinos, pursuant to OG Code 2008 Section 16(f), must disclose information to the FCU where the MLRO knows or suspects ML or FT.

STRs Related to Terrorism and its Financing (applying c. 13.2 to DNFBPs):

847. The analysis contained in section 3.7 of this report also applies to DNFBPs.

No Reporting Threshold for STRs (applying c. 13.3 & IV.2 to DNFBPs):

848. The analysis contained in section 3.7 also applies to DNFBPs. There is no specific requirement to report attempted transactions. All of the DNFBPs interviewed during the assessment stated that, in practice, any suspicious attempted transactions would be reported to the FCU.

Making of ML and TF STRs Regardless of Possible Involvement of Fiscal Matters (applying c. 13.4 and c. IV.2 to DNFBPs):

849. The reporting requirements make no reference to tax-related matters and they are therefore not excluded from the scope of the STR reporting offenses of the CJA 1990, the DTA 1996, and ATCA 2003, as discussed in section 3.

Protection for Making STRs (applying c. 14.1 to DNFBPs):

850. The discussion of Recommendation 14 in section 3.7 of this report applies equally to DNFBPs. In summary, Sections 17A(3)(a), 17B(5)(a), 17K(4)(6), and 21 CJA 1990; Sections 46(3)(a), 47(5)(a), (48)(4) and (6) DTA, 1996; and Sections 12 and 15 ATCA provide broadly-worded protection from any liability for breach of a restriction on disclosure of information imposed by statute or otherwise. However, the provisions are not sufficiently explicit to comply with the international standard.

[64] The data for CSPs include cases in which CSPs and TSPs are the same or a closely-related business.

Prohibition Against Tipping-Off (applying c. 14.2 to DNFBPs):

851. The provisions discussed in section 3 addressing tipping-off apply equally to DNFBPs. Specification of the circumstances in which a person would commit an offense by tipping off rather than directly prohibiting it apply equally to DNFBPs.

Establish and Maintain Internal Controls to Prevent ML and TF (applying c. 15.1, 15.1.1 & 15.1.2 to DNFBPs):

852. The critique under section 3.7 of this report applies equally to DNFBPs. All DNFBPs interviewed advised they could produce written internal guidelines for AML and CFT.

Independent Audit of Internal Controls to Prevent ML and TF (applying c. 15.2 to DNFBPs):

853. Dealers in precious metals, dealers in precious stones, and real estate agents advised assessors they do not routinely have an independent audit function for the testing of compliance of ML and FT systems and controls, policies, and procedures. Advocates have a self-audit system as outlined in the IOM Law Society's Guidance Notes, the report of which is signed off by an independent auditor without on-site assessment.

Ongoing Employee Training on AML/CFT Matters (applying c. 15.3 to DNFBPs):

854. As required under paragraph 22 of the AML Code 2008, DNFBPs' training procedures are implemented pursuant to the relevant Codes and in line with the discussion in section 3.7. All DNFBPs interviewed advised assessors of some level of initial and ongoing training of all staff.

Employee Screening Procedures (applying c. 15.4 to DNFBPs):

855. All DNFBPs interviewed advised that they apply some level of screening procedures for employees, in accordance with the requirement under paragraph 21 of the AML Code 2008. CSPs and TSPs are subject to fit and proper requirements under the FSC provisions while assessors were advised during interviews with terrestrial and on-line casinos that all employees undergo rigorous fitness and proprietary screening by the licenseholder.

Additional Element—Independence of Compliance Officer (applying c. 15.5 to DNFBPs):

856. The discussion in section 3.7 of this report applies equally to DNFBPs pursuant to Paragraph 20 of the Code 2008 and Section 16 of OG Code 2008

Special Attention to Countries Not Sufficiently Applying FATF Recommendations (c. 21.1 & 21.1.1):

857. The critique in section 3.6 of this report applies equally to DNFBPs. The assessors were advised during interviews that in practice, CSPs, TSP, lawyers, accountants, and casinos took into account the country of origin when assigning and profiling risk and did not limit their analysis to Schedule 2 of the AML Code 2008 and Schedule 1 of the OG Code 2008.

Examinations of Transactions with no Apparent Economic or Visible Lawful Purpose from Countries Not Sufficiently Applying FATF Recommendations (c. 21.2):

858. DNFBPs, other than on-line casinos, are subject to the provisions of the AML Code 2008, as discussed in Section 3.7 of this report. No provision to pay special attention to transactions which appear to have no economic purpose is contained in OG Code 2008, most likely due to the nature of the industry. However, licenseholders subject to the provisions of OG Code 2008 are required pursuant to Section 5 to carry out a risk assessment and records are to be kept for a minimum of six years in line with Section 13.

Ability to Apply Counter Measures with Regard to Countries Not Sufficiently Applying FATF Recommendations (c. 21.3):

859. The discussion in Section 3.7 applies equally to all DNFBPs.

4.2.2. Recommendations and Comments

- Clarify the position of legal privilege in relation to ML and FT issues and STR reporting in a manner supportive of the AML/CFT system.
- The authorities should continue their efforts, through awareness raising and otherwise, to increase the effectiveness of STR reporting by DNFBPs, particularly for those categories that rarely report suspicions.
- The authorities should amend the law to extend the protection for persons reporting suspicions to the FIU to cover all aspects in the international standard and limit the protection to reporting in good faith.
- The authorities should consider introducing measures to ensure the confidentiality, including in Court proceedings, of persons reporting suspicions to the FIU.
- The authorities should introduce a requirement in law, regulation, or other enforceable means 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 authorities should amend the law to require the reporting of suspicious attempted transactions.

4.2.3. Compliance with Recommendation 16

	Rating	Summary of factors relevant to s.4.2 underlying overall rating
R.16	**PC**	• No requirement to report attempted suspicious transactions. • Requirement for an independent audit function does not explicitly include AML/CFT within its scope.

		• Low levels of STR reporting by some categories of DNFBPs. • Protection for those reporting suspicions not fully in line with international standard. • Effectiveness of implementation of the supplemental provisions of the AML Code 2008 could not be assessed as they were adopted subsequent to the on-site visit (other than CSPs and TSPs which were already subject to Part 9 of the FSC Rule Book from August 2008).

4.3. Regulation, Supervision, and Monitoring (R.24-25)

4.3.1. Description and Analysis

Introduction

CSPs and TSPs

860. CSPs and TSPs are authorized and supervised by the FSC pursuant to the FSA 2008 and are relevant businesses under Schedule 1 of the AML Code 2008. For AML/CFT purposes, they are also subject to the FSC Rule Book 2008 and the guidance contained in the Handbook 2008. All CSPs and TSPs interviewed during the assessment reported having had on-site inspections from the FSC within the past 18 months and indicated full awareness of their obligations in relation to suspicious transaction reporting and CDD obligations.

Lawyers and legal professionals

861. The provisions of Section 3(2)(c) Advocates Act 1995 provide that the IOM Law Society has the power to 'initiate prosecutions against advocates or other persons for the breach of any enactment relating to the practice of law'. In addition, Section 16 of the Advocates Act 1976 provides the Law Society with the power to make practice rules "regulating the professional practice, conduct, and discipline of advocates". These powers make the Society the supervisory body for the legal profession with respect to AML/CFT matters. In conducting this function, and in particular with respect to the drafting of AML/CFT guidelines for its members, the Society works in close collaboration with the DHA, with which it is currently formalizing an MOU. The Society had issued guidance notes for its members with respect to the AML Code 2007, as well as a typologies report outlining various relevant money laundering techniques used by criminals. The Society has also organized a number of AML/CFT seminars for its members.

862. The IOM Law Society, Criminal Justice (Money Laundering) Code 2007 Guidance Notes were issued on August 1, 2008. In addition to the general sanctions for violations of the AML/CFT obligations contained in the then-applicable AML Code 2007 and the CJA 1990, disciplinary procedures before an independent Advocates Disciplinary Tribunal may be instituted against advocates. Disciplinary sanctions may include a reprimand, a fine and, in serious cases, suspension or revocation of the advocate's admission.

863. The Society conducts its supervisory functions through 'advocate's certificates', which are required to be filed with the Society by each member on an annual basis, stating that the firm has in place AML procedures sufficient to satisfy all existing AML/CFT requirements. The certificate is endorsed by a partner of the firm as well as the accounting firm appointed to audit the law firm. The accountant's endorsement, however, is not based on an onsite examination of the firm but on information furnished by the respective firm. While the Society plans to revise the accountant's statement to be more explicit, it has not yet conducted full on-site audits of lawyers for AML/CFT purposes. As indicated above, draft legislation allowing for onsite audits of law firms for AML/CFT purposes was being discussed before Tynwald at the time of the assessment.[65] While registered legal practitioners are subject to the same AML/CFT obligations as advocates, only the latter are subject to supervision by the Society. Legal Practitioners are obliged under the Legal Practitioners Registration Act 1986 to register with the Chief Registrar, this registration being valid for a 12 month period. As with other DNFBPs that are not regulated by a professional body, supervisory responsibility for AML/CFT matters for registered legal professionals rests with the DHA.

Accountants

864. At the time of the on-site visit, the DHA had been in dialogue with the professional accounting bodies regarding the application of AML/CFT requirements to the accounting profession. Once finalized, it is expected that there will be a requirement for an annual AML/CFT compliance report from the accounting bodies to the DHA. The UK-based Consultative Committee of Accounting Bodies (CCAB) issued AML/CFT guidance in December 2007 on behalf of its six professional accountancy member bodies. Two of the six bodies, The Institute of Chartered Accountants in England and Wales and The Association of Chartered Certified Accountants, cover the majority of the accounting profession in the IOM. However, the guidance, while useful, is primarily UK-based and not IOM specific. The authorities indicated that they plan to adapt it for IOM purposes. However, the assessors are not in a position to assess the effectiveness of measures taken subsequent to the on-site visit.

Dealers in precious metals or stones

865. Similar to other DNFBPs not supervised by professional bodies, dealers in precious metals and dealers in precious stones are required to register with the DHA. Further, all IOM dealers in high-value goods and other local businesses with a turnover in excess of GBP64,000 per annum are among those businesses that have to register for Value Added Tax (VAT) with IOM Customs and Excise, which conducts visits to them to ascertain compliance with the laws and regulations, including in relation to AML/CFT. The assessors were advised by Customs and Excise, and confirmed during interviews with dealers in high-value goods, that an active awareness-raising campaign in relation to the obligations pursuant to the AML Code 2007 had been underway, specifically aimed at businesses dealing in goods and accepting large cash payments. The awareness-raising exercise involved mailshots and leaflets to relevant businesses concerning their AML/CFT obligations, press releases and adverts in the local media, posters at the airport and port, free seminars hosted by the FSC and media interviews.

[65] The Advocates (Amendment) Bill completed passage through Tynwald in May 2009 and is awaiting Royal Assent.

Casinos

866. The Gambling Supervision Commission (GSC) has conducted two on-site assessments (with a further 10 scheduled) and 11 desk top reviews in 2008 for online casino operations. Additionally, the GSC undertakes weekly on-site checks covering a range of aspects of the business of the one terrestrial casino. External independent audits of the casino are also conducted. Training has been outsourced to a competent service provider. At the time of the assessment, the GSC was in the process of issuing guidance notes[66] in relation to the Criminal Justice (Money Laundering-Online Gambling) (No.2) Code 2008 to replace the 2002 Guidance Notes. In line with the growth in this sector, consideration will need to be given to staffing levels and capacity generally of the GSC to deal with the increased workload.

Other DNFBPs

867. At the time of the on-site visit, the DHA had issued guidance for the DNFBPs not within the mandate of the FSC or GSC to assist with the implementation of the AML Code 2007 and is engaging with the various sectors identified to develop a methodology and approach to ensure compliance. The DHA advised that this work is based on risk assessments of ML and FT vulnerabilities across the relevant sectors. The DHA has been working closely with the FSC in raising awareness in the sectors covered, through media campaigns and seminars. The assessors are not in a position to assess the effectiveness of measures taken subsequent to the on-site visit.

Regulation and Supervision of Casinos (c. 24.1, 24.1.1, 24.1.2 & 24.1.3):

868. The terrestrial and on-line casinos are authorized, regulated, and supervised by a competent authority, the Gambling Supervision Commission (GSC), pursuant to the CJA1990, Online Gambling Regulation Act 2001, and the Casino Act 1986. The terrestrial casino is a 'relevant business' pursuant to the AML Code 2008 and the on-line casinos are subject to the Criminal Justice (Money Laundering–Online Gambling) (No. 2) Code 2008 with associated guidance notes—in draft form at the time of the assessment—to replace the revoked Code 2002 guidance notes.

869. Powers to monitor and sanction financial institutions as described in section 3.10 of this report apply to the terrestrial casino. Powers to monitor and sanction on-line casinos are contained in the Online Gambling Regulation Act 2001 Section 18 and in Section 20 of the Criminal Justice (Money Laundering–Online Gambling) (No.2) Code 2008. Criminal sanctions, for a natural person and legal person, can apply pursuant to the Section 18 of the Act and Section 20 of the Code 2008 with fines, convictions, or custody or a combination thereof.

870. Fit and proper tests are conducted by the GSC at the license application stage and are ongoing after authorization. Further checks are undertaken with the police, Customs and Excise, and FSC, together with financial background checks, reference checking, and interviews with key company personnel.

[66] Guidance Notes published subsequent to the assessment in April 2009.

Monitoring Systems for Other DNFBPs (c. 24.2 & 24.2.1):

871. Powers to monitor and sanction for financial institutions discussed in section 3.10 of this report apply also to DNFBPs. CSPs and TSPs are required to implement effective systems for monitoring and ensuring compliance with AML/CFT requirements. Staffing resources of the FSC appear generally adequate in relation to the supervision of CSPs and TSPs.

872. Advocates are part of a self-certification system as described previously in section 4, within the mandate of the IOM Law Society. Registered legal practitioners do not fall within the mandate of the Society and a void currently exists as regards their monitoring. The DHA supervise other DNFBPs, including dealers in precious metals, dealers in precious stones, and real estate agents, and discussion is underway with two accounting bodies for the AML/CFT supervision of the accounting profession.

873. The DHA is proposing amendments to the CJA 1990 for specific powers to hold a compulsory register and the power to fine for non-compliance with registering; providing false information; accepting cash transaction over EUR15,000 without registering for that purpose; and the right of direct access to records and procedures. The proposed amendments would also benefit the supervision by the accounting and legal bodies as these bodies would be approved by DHA in statute so that the bodies could be empowered to regulate members on behalf of DHA, instead of being reliant on the ultimate sanction of being expelled from the professional body. Relevant provisions of the POCA 2008, in effect from August 1, 2009, provide for powers to issue rules that will be legally binding on accounting and legal firms and empower specific regulation of DNFBPs.

Guidelines for DNFBPs (applying c. 25.1):

874. While not binding, a number of categories of DNFBPs have been issued with guidance on implementing and complying with their AML/CFT requirements. The IOM Law Society; DHA, and FSC issued guidance pertaining to the implementation of the AML Code 2008. The GSC has developed guidance notes to support the Criminal Justice (Money Laundering–Online Gambling) (No.2) Code 2008. All are useful documents which, as reported to the assessors by DNFBPs interviewed, have been well received by the relevant parties.

875. With regard to casinos, the analysis for Recommendation 24 set out the basis on which the GSC conducts its supervision for both terrestrial and online casinos. Given the growth in the online business, there is a need for the GSC to assess the adequacy of its staffing capacity and specialist skills base, including in the information technology area, to ensure that it is well positioned to deal with further expansion of the gambling sector. For the DHA, depending on the outcome of the current initiatives to design and implement an AML/CFT system appropriate to the remaining DNFBPs, there might be a need to assign additional resources to ongoing AML/CFT supervision and liaison with the SROs for the legal and accountancy professions.

4.3.2. Recommendations and Comments

The authorities should:

- Provide for and implement a system of regular and full audits for advocates based on onsite visits to monitor more closely the level of compliance with their AML/CFT obligations.

- Ensure that registered legal practitioners are supervised to ensure their compliance with the provisions of the AML Code 2008.
- Finalize the agreement between the DHA and the professional accounting bodies, issue guidance adapted to the IOM's AML/CFT requirements, and implement an AML/CFT on-site supervisory regime for the industry.
- Formalize the basis for on-site assessments for DNFBPs that do not fall within the mandate of the FSC, GSC, or the IOM Law Society.
- Proceed with planned legislative amendments to provide the DHA with adequate powers in undertaking registration and regulation for AML/CFT purposes of DNFBPs within its mandate and provide the DHA with resources consistent with that mandate.
- Assess the adequacy of the GSC's staffing capacity and specialist skills base to ensure it is well positioned from an AML/CFT perspective to deal with the expected growth in on-line and terrestrial casino business.

4.3.3. Compliance with Recommendations 24 & 25 (criteria 25.1, DNFBP)

	Rating	Summary of factors relevant to s.4.3 underlying overall rating
R.24	**PC**	• Implementation of AML/CFT measures for DNFBPs, other than CSPs, TSPs, and most lawyers, is still being developed. • Registered legal practitioners are not adequately covered by the AML/CFT requirements. • The powers of the DHA to perform an AML/CFT supervisory role had not come into legal affect. • Additional supervisory resources needed for the DHA and GSC, including for the latter additional specialist skills to deal with on-line casino systems.
R.25	**LC**	Section-specific rating would be: LC • Up-to-date guidance had not yet been issued by the GSC at the time of the assessment. • Guidance for accounting professionals has not been adapted to the IOM requirements.

4.4. Other Non-Financial Businesses and Professions—Modern-Secure Transaction Techniques (R.20)

4.4.1. Description and Analysis

Introduction

876. The FATF Recommendations and Methodology provide the following examples of businesses or professions to which countries 'should consider' applying AML/CFT requirements: dealers in high value and luxury goods, pawnshops, gambling, auction houses, and investment advisers. The assessors confirmed that the IOM authorities, and the DHA in particular, have been giving consideration to this area based on analysis of the vulnerability of such businesses to abuse for ML or FT purposes.

Other Vulnerable DNFBPs (applying R. 5, 6, 8-11, 13-15, 17 & 21 c. 20.1):

877. Pursuant to Schedule 1, Section 24 of the AML Code 2008 applies its provisions to businesses dealing in goods of any description including:

- dealing as an auctioneer; and
- whenever a transaction involves accepting cash payment of EUR15,000 or more.

878. The DHA has been engaged with relevant sectors identified other than DNFBPs to develop a methodology and approach to ensure compliance with the requirements of the AML Code 2008. The DHA has issued relevant guidance to such enterprises on money laundering and terrorist financing prevention and has undertaken a concentrated awareness campaign in conjunction with the FSC and Customs and Excise.

879. All local high value dealers (HVD) and other local businesses with a turnover in excess of GBP64,000 per annum have to register for Value Added Tax (VAT) with IOM Customs and Excise who then visit these businesses to ascertain compliance with the laws and regulations, including requirements pertaining to AML and CFT. During July and August 2008 IOM Customs and Excise conducted visits to all the IOM's HVDs, numbering around 70 premises, carrying out face-to-face consultations about the risks associated with accepting large cash payments and the responsibilities of the businesses under the IOM's AML Code should they accept cash in excess of EUR15,000. Customs and Excise staff advised the assessors that, in undertaking visits to inspect traders' books and records, they can identify transactions that exceed the EUR15,000 threshold and if the trader has failed to comply with the requirements of the AML Code 2008, they would report such cases to the FCU for appropriate action.

Modernization of Conduct of Financial Transactions (c. 20.2):

880. The AML Code 2008 applies to all business dealing in goods that accept cash payments over EUR15,000 and, as of June 1, 2008, the carriage of cash to the equivalent of EUR10,000 or more into or from the IOM requires the completion of a cash declaration form. Failure to declare cash above the threshold is subject to financial penalties by Customs and Excise.

881. The IOM has a highly-developed financial system, with modern and secure techniques for conducting financial transactions and a low dependence on cash usage. A full range of payment systems is available, tied closely to those of the UK.

4.4.2. Recommendations and Comments

- The authorities should proceed with their program of awareness-raising to determine what categories of NFBP should be within the scope of the AML/CFT requirements.

4.4.3. Compliance with Recommendation 20

	Rating	Summary of factors underlying rating
R.20	**LC**	• Consideration not yet concluded on the application of AML/CFT requirements to other NFBPs.

5. LEGAL PERSONS AND ARRANGEMENTS & NON-PROFIT ORGANIZATIONS

5.1. Legal Persons—Access to Beneficial Ownership and Control Information (R.33)

5.1.1. Description and Analysis

Legal Framework:

882. As outlined in section 1 of this report, the IOM has three sets of laws governing legal persons, namely the Companies Act 1931–2004, the Companies Act 2006, and the Limited Liabilities Act 1996. While the first two Acts allow for the incorporation of a wide range of corporate entities, including Companies Limited by Shares, Companies Limited by Guarantee, Companies Limited by Guarantee and having a Share Capital, Unlimited Companies and Protected Cell Companies, the latter provides for and regulates the incorporation of Limited Liability Companies (LLCs).

Measures to Prevent Unlawful Use of Legal Persons (c. 33.1):

883. According to Section 74 (3) Companies Act 2006, any company incorporated under the Act has to have a registered agent that holds a license pursuant to the FSA 2008. The name as well as the address of the registered agent has to be filed with the Companies Registry.

884. With respect to 1931 Companies and LLCs, no general requirement exists to utilize the services of a licensed corporate service provider. In situations where such a company uses the premises or utilizes company management or nominee services offered by a person who does not conduct such activities 'by way of business', that person would not be covered by the FSA 2008 and would therefore not be subject to the obligations under the AML Code 2008 or FSA Rule Book 2008.

885. In considering how the IOM complies with the FATF Recommendations in this area, which call for persons conducting such activities 'as a business' to be subject to AML/CFT requirements, the assessors note that the term 'by way of business' is not defined anywhere in the FSA 2008. The authorities stated that the term would be interpreted in line with the common understanding of the words and past interpretations by the Courts. Assessors were shown a number of letters from the FSC to various individuals, responding to requests for determination as to whether or not an activity would be considered to be conducted 'by way of business'. The facts considered by the FSC in making that determination include whether the activity in question formed part of the individual's core business, whether the individual 'held itself out' and indicated a willingness to accept new business in the respective area, whether the person had commercial intention in conducting the activity, whether the activity was conducted through a company, the overall number of appointments, and whether the individual received a remuneration and, if so, what amount.

886. In cases where 1931 Companies and LLCs choose to utilize the services of a person who conducts company management and nominee services 'by way of business', the Regulated Activities Order 2008 introduced in August 2008 a number of exclusions from the licensing requirement. In particular (1) a person providing or arranging for premises for use as a registered office in his capacity as a landlord or property manager or estate agent; (2) an advocate or registered legal practitioner or accountant providing company management or nominee services, or acting as registered agent or providing a registered office address wholly incidental to the giving of legal

advice given or to a professional activity undertaken; and (3) an individual acting as a director or secretary of a company wholly and beneficially owned by him or a close relative, are not considered 'regulated activities' pursuant to the FSA 2008 and are therefore excluded from the licensing obligation. While the scope of the AML Code 2008 covers such excluded corporate service providers within AML/CFT requirements, persons excluded from the list of 'regulated activities' are not subject to FSC supervision and their level of compliance with the obligations of the AML Code 2008 is, therefore, not monitored by the FSC.[67] The position in respect of advocates and accountants is discussed elsewhere in the report.

887. Finally, while activities pursuant to the Financial Services (Exemptions) Regulations 2008 are considered to be regulated activities, they are exempted from the licensing requirements of the FSA 2008. The most notable exempted regulated activity is the acting, by way of business, as a director for less than 10 companies (de minimis exemption). As is the case for excluded persons, persons carrying out exempted activities are covered by the AML Code 2008 but are still not subject to any monitoring for compliance with those obligations. In summary, while all 2006 Companies, through the licensed registered agent requirement, are subject to the obligations under the AML Code 2008, 1931 Companies and LLCs are covered only in situations where the director, secretary, or the person providing a registered office or acting as registered agent provides such services by way of business. The statistics maintained by the FSC as well as the Companies Register suggest that, as of December 2007, only about 70 percent of all 1931 Companies and LLCs were administered by licensed corporate service providers. Therefore, about 30 percent of those companies would not be subject to requirements to identify, verify, and maintain beneficial ownership information. The authorities stated that most of those companies would be local manufacturing and commercial companies and thus the registered shareholders would most likely also be the beneficial owners.

888. With respect to the other 70 percent as well as all 2006 Companies, licensed corporate service providers are required with respect to all clients to "identify who is the beneficial owner of the applicant" and to "take reasonable steps to verify the identity of those persons, using relevant information or data obtained from a reliable source" in accordance with AML Code 2008 paragraph 5. The Code defines 'beneficial owner' as 'the natural person who ultimately owns or controls the applicant for business or on whose behalf a transaction or activity is being conducted'. With respect to legal persons, the requirement extends to any natural person who ultimately owns or controls, whether through direct or indirect ownership or control, more than 25 percent of the shares or voting rights in the legal person, or who otherwise exercises control over the management of the legal person. In addition, licensed corporate service providers are also subject to the FSC's Rule Book 2008, Part 9 of which deals with AML/CFT and was brought into effect on August 1, 2008. The Rule Book requires licenseholders to identify and take reasonable measures to verify the identity of the beneficial owner in all cases.

---

[67] Prior to August 1, 2008, corporate service providers were subject to the Corporate Service Providers Act 2000, which contained exemptions from the requirement to hold a license but did not provide for any exclusion from AML/CFT requirements. The introduction of such exclusions by the Regulated Activities Order 2008 gave rise to the need to include the excluded providers within the scope of the AML Code 2008 in order to maintain the status quo.

Access to Information on Beneficial Owners of Legal Persons (c. 33.2):

889. All legal entities incorporated in the IOM obtain legal personality upon registration with the Companies Registry. Although the Companies Registry does not record information on beneficial ownership, it contains the names and addresses of registered agents, the address of registered IOM offices, and with respect to 1931 Companies and LLCs also the names of directors, secretaries, and shareholders. All information and documentation held at the Companies Registry is freely accessible to the public, including online.

890. 2006 Companies have an obligation to file any amendments to their articles of agreement with the Company Registry within one month, for which purpose a change of the registered office or agent is deemed a change of the company's articles. 1931 Companies and LLCs have to notify the Companies Registry within one month of any chances to any registered information. In addition, all companies have to file an annual return as outlined in section 1 of this report.

891. FSA 2008 Schedule provides the FSC with a wide range of inspection and investigation powers. Pursuant to the relevant provisions, the FSC may inspect books, accounts, and documents, request any information required to perform its function under the FSA 2008 and, subject to a court order, issue subpoenas and production orders and seize and copy documents. Those powers do not, however, extend to corporate service providers that are either excluded from the FSA 2008 or that do not conduct such activities 'by way of business' and thus are not covered by the FSA 2008 as outlined above. In cases involving such persons, the general law enforcement powers as outlined under section 2 of this report could be used to obtain beneficial ownership information on legal persons.

Prevention of Misuse of Bearer Shares (c. 33.3):

892. The Companies Act 2006 expressly prohibits the issuance of bearer shares and even makes it an offense to do so. By comparison, Section 71 of the Companies Act 1931-2004 voids any provisions in the memorandum of association of companies that would allow for the issuance of bearer shares but validates any bearer shares issued before enforcement of the provision. However, since 2004 no rights attached to any such bearer shares may be exercised without conversion of the share into a registered share. At the time of the assessment, about 1.3 million bearer shares issued through 109 companies and representing a nominal share value of GBP 940,904 were still outstanding.

893. All IOM companies are required to keep a register at the company's registered IOM office stating the full names and addresses of all shareholders and members, whereby the register is prima facie evidence that legal title in the share vests in the registered person.

Additional Element—Access to Information on Beneficial Owners of Legal Persons by Financial Institutions (c. 33.4):

894. Financial institutions have full access to all information and documentation held at the Companies Registry but, as noted, the Registry does not maintain information on beneficial ownership. As described in section 3 of this report, financial institutions are required to identify beneficial owners and take reasonable steps to verify their identity. However, no specific measures

are in place to facilitate access by financial institutions to beneficial ownership and control information, so as to allow them to more easily verify the customer identification data.

Analysis:

895. Pursuant to AML Code 2008 paragraph 5, licensed corporate service providers are required to identify in all cases the natural person ultimately owning or controlling a customer or a person on whose behalf a transaction is being conducted as well as any person who exercises ultimate effective control over a legal person, and to take reasonable steps to verify the identity of those persons based on reliable information. In addition, as of August 1, 2008 all persons and entities licensed pursuant to the FSA 2008, including corporate service providers, are subject to the provisions of Part 9 of the FSC Rule Book, which requires the identification of the beneficial owner in all cases. In practice, all practitioners interviewed by the assessors indicated that they always identify the beneficial owner.

896. As outlined above, 1931 Companies and LLCs are not required to utilize the services of licensed company service providers and in about 30 percent of all cases, which amounts to about 9,300 companies, choose not to do so. While it is not required under the FATF standard that all companies are linked with a professional service provider, it is required that countries have measures in place to ensure adequate transparency concerning the beneficial ownership and control of legal persons and that the competent authorities can obtain and have access to adequate, accurate, and current beneficial ownership information on all legal entities. The Companies Register also does not maintain any beneficial ownership information for such companies. While the authorities may rely on law enforcement powers to obtain beneficial ownership information in such cases, it is questionable how complete, accurate, and current any beneficial ownership information would really be.

897. With respect to 1931 Companies and LLCs utilizing the services of excluded or exempted corporate service providers, the effective implementation of the measures set out in the AML Code 2008 by exempted and excluded corporate service providers could not be demonstrated for purposes of this assessment in light of the fact that those persons are not subject to any supervision by the FSC. The position in respect of monitoring of advocates and accountants is discussed elsewhere in this report.

898. The authorities are advised to put in place measures to ensure that accurate, complete and current beneficial ownership information is available for all 1931 Companies. One approach would be to require the filing of beneficial ownership information with the Company Registry in cases where a licensed corporate service provider is not utilized.

899. While bearer shares still exist with respect to IOM companies, there are measures in place as described above to limit the risk that bearer shares could be misused for ML or FT purposes.

5.1.2. Recommendations and Comments

- The authorities should seek to put in place measures to ensure that accurate, complete, and current beneficial ownership information is available for all 1931 Companies and LLCs.

- The authorities should consider extending the formal monitoring of corporate service providers for compliance with the requirements of the AML Code 2008 to include those "exempted" or "excluded" from the licensing requirements of the FSA 2008.

5.1.3. Compliance with Recommendations 33

	Rating	Summary of factors underlying rating
R.33	**LC**	• For about 30 percent of the 1931 Companies and LLCs, it could not be determined that accurate, complete, and current beneficial ownership information is available.

5.2. Legal Arrangements—Access to Beneficial Ownership and Control Information (R.34)

5.2.1. Description and Analysis

Legal Framework:

900. Trusts have been recognized under IOM law for many years, whereby the Trustee Act 1961 and its subsequent amendments are the main pieces of legislation governing such legal arrangements. In addition, the common law principles of trust law and equity are applied and recognized by the IOM Courts insofar as they are not contrary to statutory law or local precedent. Express trusts, implied trusts, resulting trusts, as well as constructive trusts are all recognized and utilized in the IOM. Since 1996 IOM law also allows for the enforcement of purpose trusts provided that the trust purpose is certain, reasonably enforceable, and not contrary to the law.

Measures to Prevent Unlawful Use of Legal Arrangements (c. 34.1):

901. Pursuant to the Regulated Activities Order 2008, any person who, by way of business, acts as a sole or other trustee in relation to an express trust, who provides trust administration services in relation to an express trust, who acts as trust corporation or as protector in relation to an express trust, or an enforcer in relation to a purpose trust falls under the licensing requirement pursuant to FSA 2008. 'Protector' is defined as a person other than a trustee who, as the holder of an office created by or under the terms of the trust, is authorized or required to participate in the administration of the trust.

902. Any person providing such services other than 'by way of business' would not be required to obtain a license pursuant to FSA 2008. As indicated in the analysis under Recommendation 33 above, there is no definition of the term 'by way of business'.

903. In addition, the Regulated Activities Order 2008 provides for a number of exclusions from the licensing requirement for trustees. For example, advocates or registered legal practitioners or accountants carrying out any of the activities listed in the Regulated Activities Order 2008 as wholly incidental "to the giving of legal advice or the undertaking of a professional activity" are not considered 'regulated activities' and would therefore be excluded from the licensing obligation. While persons conducting an activity excluded from the licensing requirement are subject to the full

range of measures provided for in the AML Code 2008, they are not subject to any monitoring for compliance with the obligations under the AML Code 2008.[68]

904. Moreover, while activities pursuant to the Financial Services (Exemptions) Regulations 2008 are considered to be regulated activities, they are exempted from the licensing requirements of the FSA 2008. The most notable exempted regulated activity is acting, by way of business, as a trustee for less than 10 legal arrangements (de minimis exemption). Other exemptions relate to private trust companies that were set up solely for one specific trust and where the trust is question is administered by a license holder as well as to certain testamentary and small domestic trusts. Just like trust service providers excluded from the list of regulated activities pursuant to the Regulated Activities Order 2008, since December 2008 persons carrying out such exempted activities are covered by the AML Code 2008 but are still not subject to any monitoring for compliance with those obligations. Prior to December 2008, persons conducting activities exempted from the licensing requirement were subject to the obligations under the previous AML Code and therefore were obliged to obtain, verify, and maintain information on the identity of legal entities' beneficial owners.

905. As already outlined above, paragraph 5 of the AML Code 2008 requires covered entities with respect to all clients to "identify who is the beneficial owner of the applicant" and to "take reasonable steps to verify the identity of those persons, using relevant information or data obtained from a reliable source". The Code defines 'beneficial owner' as 'the natural person who ultimately owns or controls the applicant for business or on whose behalf a transaction or activity is being conducted'. With respect to legal arrangements, the provision requires identification of the trustees or any other persons controlling the client. In addition, Part 9 of the FSC Rule Book requires to identify the beneficial owner and to take reasonable measures to verify the identity in all cases.

906. As the exclusions or exemptions under the FSA 2008 do not require permission by or notification to the FSC, the authorities do not maintain statistics or estimates of the number of trustees operating in the IOM that are not covered by the FSA 2008. The authorities stated, however, that they would occasionally receive requests for determination as to whether or not the requesting individual would fall under the scope of FSA 2008.

Access to Information on Beneficial Owners of Legal Arrangements (c. 34.2):

907. As already outlined in section 1 of this report, trusts are not subject to any registration or filing requirements. While licensed trust service providers have to file an annual return with the FSC indicating the number of trusts administered, the return does not typically contain any information pertaining to individual trusts or the trust accounts.

908. With respect to persons conducting any regulated activity by way of business, FSA 2008 Schedule 2 provides the FSC with a wide range of inspection and investigation powers. Pursuant to the relevant provisions, the FSC may inspect books, accounts, and documents, request any

[68] Prior to August 1, 2008, trustees were subject to the Corporate Service Providers Act 2000, which contained exemptions from the requirement to hold a license but did not provide for any exclusion from AML/CFT requirements. The introduction of such exclusions by the Regulated Activities Order 2008 gave rise to the need to include the excluded trustees within the scope of the AML Code 2008 in order to maintain the status quo.

information required to perform its function under FSA 2008 and, subject to a court order, issue subpoenas and production orders and seize and copy documents.

909. Those powers do not, however, extend to trust service providers either excluded from the FSA 2008 or those that do not conduct such activity 'by way of business' and are therefore not covered by the FSA 2008 as outlined above. For cases involving such persons, the general law enforcement powers as outlined under section 2 of this report would apply.

910. As of December 2007, 22,785 trusts were administered by licensed IOM trust service providers. The authorities could not provide information or an estimate on the number of trusts falling outside of the scope of or excluded from the provisions of FSA 2008.

Additional Element—Access to Information on Beneficial Owners of Legal Arrangements by Financial Institutions)(c. 34.3):

911. No specific measures are in place to facilitate access by financial institutions to beneficial ownership and control information, so as to allow them to more easily verify the customer identification data.

Analysis:

912. For all legal arrangements administered by licensed trust service providers, AML Code 2008 paragraph 5 provides that trust service providers have to identify in all cases the natural person ultimately owning or controlling a customer or a person on whose behalf a transaction is being conducted as well as any person who exercises ultimate effective control over a legal person, and to take reasonable steps to verify the identity of those persons based on reliable information. In addition, as of August 1, 2008, all licensed trust service providers are also subject to the provisions of Part 9 of the FSC Rule Book, which requires the identification of the beneficial owner in all cases. In practice, all practitioners interviewed by the assessors indicated that they always identify the beneficial owner.

913. For legal arrangements administered by trustees not covered by FSA 2008, the provisions of the AML Code 2008 do not apply. While the enforcement and investigative powers granted to the FSC seem to be substantial, they do not apply to activities excluded from the licensing requirements of the FSA 2008 or to persons providing trust services other than 'by way of business'. In any case, it is questionable how complete, accurate, and current any beneficial ownership information held by such unregulated and unsupervised trustees would really be.

914. For legal arrangements administered by trustees exempted or excluded from the licensing requirement of the FSA 2008, the effective implementation of the measures as set out in the AML Code 2008 could not be demonstrated for purposes of this assessment in light of the fact that those persons are not subject to any supervision by the FSC. The position in respect of monitoring of advocates and accountants is discussed elsewhere in this report.

915. While there is a general obligation under the Trustee Act 1961 for the trustee to ensure that any distributions are made properly and according to the requirements of the particular trust (which means he has to ensure that distributions are made to the right beneficiary), there is no obligation to maintain any records of the identity of the beneficiary or to verify the identity. The obligation to

identify the beneficiary prior to making any distributions does not extend to other persons falling under the definition of beneficial owners, such as protectors of trusts or other persons exercising ultimate effective control over a legal arrangement, but merely extends to the beneficiaries.

5.2.2. Recommendations and Comments

- The authorities should seek to put in place measures to ensure that accurate, complete and current beneficial ownership information is available for legal arrangements administered by a trustee who is not covered by the licensing requirements of FSA 2008.

- The authorities should consider extending the formal monitoring of trust service providers for compliance with the requirements of the AML Code 2008 to include those "exempted" or "excluded" from the licensing requirements of the FSA 2008.

5.2.3. Compliance with Recommendations 34

	Rating	Summary of factors underlying rating
R.34	**LC**	• 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.

5.3. Non-Profit Organizations (SR.VIII)

5.3.1. Description and Analysis

Introduction

916. IOM charitable bodies are registered with the General Registry under the Charities Registration Act 1989. The Chief Registrar will refuse registration if satisfied that the institution is not established for charitable purposes or that it does not have a substantial and genuine connection with the IOM. Any institution in the IOM that takes or uses any name, style, title or description implying or otherwise holding itself out to be a charity is guilty of an offense unless it is registered or exempt from registration. Exemptions for registration can be issued pursuant to Section 2(3) of the Act which provides that bodies may be exempt from registration requirements by regulation made by the Deemsters which require Tynwald approval. The Religious Charities Regulations 1999 exempt a number of religious charitable bodies from the need to register under the 1989 Act and more generally The Charities (Exemption) Regulations 2008 similarly exempt certain institutions which comply with conditions set out in the Regulations to the satisfaction of the AG.

917. As of September 2008, approximately 675 charities were registered with the Chief Registrar, of which over 75 percent have income below GBP25,000 and over 50 percent have income below GBP5,000.

918. NPOs which do not fall within the definition of charities, primarily because they were not established for the public good, are not subject to specific legislation. They would typically include organizations established to promote sports clubs and associations, hobby clubs, or youth clubs.

Review of Adequacy of Laws & Regulations of NPOs (c. VIII.1):

919. The authorities are in the course of reviewing the adequacy of legal framework relating to NPOs. A public consultation paper was issued to invite comments on options for the registration, regulation, and monitoring of such bodies to prevent their possible use in the financing of terrorism. The IOM authorities indicated that they plan to take the comments received in response to the consultation exercise into account when they complete their consideration as to whether, on a risk-based approach, any amendment to the current legal framework is warranted.

Outreach to the NPO Sector to Protect it from Terrorist Financing Abuse (c. VIII.2):

920. The General Registry undertook a desk-top review of registered charities' objectives and mandates within the twelve months prior to the assessment visit in relation to the funding of foreign jurisdictions' charitable activities. All charities subsequently identified were individually contacted and provided with general information to raise awareness of the risks surrounding Terrorist Financing Abuse. This is in addition to the public consultation relating to the general NPO sector currently in progress.

Supervision or Monitoring of NPOs that Account for Significant Share of the Sector's Resources or International Activities (c. VIII.3):

921. Audit requirements for registered charities apply pursuant to Section 5 of the CRA 1989 (which was substituted by the Audit Act 2006). Where gross per annum income is:

- less than GBP5,000, no audit is required;
- GBP5,000 to GBP100,000, an external independent examination is required;
- GBP100,000 or above, an independent external audit is required.

However, the audit is not specifically focused on elements of ML or FT.

922. No onsite monitoring of NPOs is undertaken by the General Registry, although it undertook a desk-top review of registered charities' objectives and mandates within the twelve months prior to the assessment visit in relation to the funding of foreign jurisdictions' charitable activities.

Information maintained by NPOs and availability to the public thereof (c. VIII.3.1):

923. Every charity must register specified documents in the General Registry including a copy of the instrument by which it is established and, in the case of a body corporate, its memorandum and articles of association (Section 2 CRA 1989 and Regulation 5 C(G) Regulations 1990). Information on the purpose and objectives of the charity is available on public record in the General Registry.

924. Regulation 5(1) of C (G) Regulations 1990 also requires details to be included on the register of the names and addresses of the trustees or other persons in whom the charity is vested and, in the case of a company, the names and addresses of each of the directors. If the assets of the charity are vested in some person(s) other than the charity, then the names and addresses of those persons must also be registered. (Schedule 2 of C (G) Regulations 1990).

925. There are no such registration or documentation requirements in relation to NPOs which are not charities.

Measures in place to sanction violations of oversight rules by NPOs (c. VIII.3.2):

926. Pursuant to CRA 1989, there are provisions for imposition of criminal penalties on trustees, directors, managers, or similar officers of charitable institutions who breach the statutory obligations in relation to:

- the use of the word 'charity';
- the registration requirement;
- the preparation of accounts;
- the use of misleading names;
- the provision of information to the Attorney General; and
- the filing of documents in the General Registry.

927. Charities which are suspected of being involved in money laundering, fraud or other serious criminal activity are subject to sanctions and remedies which are available pursuant to the CJA1990.

Licensing or registration of NPOs and availability of this information (c. VIII.3.3):

928. As discussed above, charities are required to be registered with the General Registry which is a public registry.

Maintenance of records by NPOs, and availability to appropriate authorities (c. VIII. 3.4):

929. No requirement is currently in place and this matter is part of the current public consultation paper.

Measures to ensure effective investigation and gathering of information (c. VIII.4):

930. The AG has wide powers to require information to be provided and to institute inquiries in relation to an institution which is, or purports to be, established for charitable purposes. The AG can apply to the High Court for relief in cases of suspected misconduct or mismanagement; in cases where the property of the charity is to be protected, or generally in the public interest. The powers available pursuant to Sections IV and V of ATCA 2003 may be used to institute a terrorist investigation against NPOs, including registered charities.

Domestic cooperation, coordination and information sharing on NPOs (c. VIII.4.1):

931. A number of statutory gateways exist to allow cooperation and the sharing of information between law enforcement and regulatory bodies in the IOM. The measures in place do not distinguish between whether information is held on individuals, bodies corporate, bodies non-corporate, or NPOs. Such gateways and cooperative agreements are discussed elsewhere in this report.

Access to information on administration and management of NPOs during investigations (c. VIII.4.2):

932. The powers vested pursuant to Section 52 of the DTA 1996; Section 17J and Section 24 of the CJA 1990; Sections 11 and 12 and Schedule 1 of the PPPA 1998 apply.

Sharing of information, preventative actions and investigative expertise and capability, with respect NPOs suspected of being exploited for terrorist financing purposes (c. VIII.4.3):

933. In addition to the gateways in VIII 4.1, Section 56 of ATCA 2003 permits disclosure of information by any public authority for the purposes of a criminal investigation being undertaken in the IOM or elsewhere or for the purposes of criminal proceedings which have been instigated in the IOM or elsewhere.

Responding to international requests regarding NPOs - points of contacts and procedures (c. VIII.5):

934. Formal requests for assistance are made through the AG's Office, as discussed elsewhere in this report.

5.3.2. Recommendations and Comments

- The authorities should complete the current review of the NPO laws and regulations and consider, based on an FT risk assessment, the merits of expanding the current coverage of charities to include other NPOs.

- The authorities should conduct periodic vulnerability reviews and outreach to the NPO sector regarding the risk of abuse for FT purposes.

5.3.3. Compliance with Special Recommendation VIII

	Rating	Summary of factors underlying rating
SR.VIII	**LC**	• Review of NPO laws and regulations not yet complete. • Current coverage excludes NPOs that are outside the definition of charities.

6. NATIONAL AND INTERNATIONAL CO-OPERATION

6.1. National Co-Operation and Coordination (R.31 & R. 32)

6.1.1. Description and Analysis

Mechanisms for Domestic Cooperation and Coordination in AML/CFT (c. 31.1):

935. Sharing of information between the law enforcement authorities and other stakeholders is formally provided for in the relevant legislation, as shown in the table below, creating a comprehensive and controlled cooperation/information network in respect of ML/TF issues. MOUs, such as between the FSC and the FCU, further streamline the cooperative relationships between the law enforcement and regulatory authorities.

936. Coordination is ensured at different levels:

- At operational level the FCU's Strategic Board, consisting of the Chief Constable, the Collector of Customs and Excise, and the AG, sets out the law enforcement strategy and directs and oversees the coordination of the law enforcement effort with input from the police, customs, and judiciary on prevention, intelligence, and enforcement. The Strategic Board advises the DHA, the ministry responsible for developing the AML/CFT Codes with which relevant businesses are required to comply.

- At policy level, the Joint Anti-Money Laundering Advisory Group (JAMLAG), is an active forum comprising representatives of law enforcement and regulatory authorities, the financial industry, and other professionals involved in the AML/CFT effort. The authorities represented in JAMLAG include the DHA, FSC, IPA, GSC, AG, FCU, Customs and Excise, and Treasury.[69] Although its primary purpose of the committee is to provide policy advice, it is also a key consultative body in that it involves all the main stakeholders and is instrumental in determining the legislative framework.

937. At the administrative/legislative level, the Chief Secretary's Office ensures coordination between government departments and authorities. Together with the AG and DHA, the Chief Secretary fulfils an important coordinating role in the development of primary and secondary AML/CFT legislation.

Additional Element - Mechanisms for Consultation Between Competent Authorities and Regulated Institutions (c. 31.2):

938. The IPA and FSC hold regular meetings with industry representative organizations. As a matter of policy, both regulatory authorities are readily accessible to licenseholders and open to meeting them to discuss any matters, including those relating to AML/CFT issues. The IPA and FSC

[69] The Office of Fair Trading has subsequently been added to the authorities which attend JAMLAG.

are co-chairs of JAMLAG, which meets regularly to discuss AML/CFT issues and developments and at which all relevant divisions and departments attend. Industry bodies such as the Compliance Institute and Securities Institute also provide additional opportunities and fora in which AML/CFT co-operation is further fostered.

939. Coordination and consultation is also provided for in legislation. Section 50(3) of IA 2008 provides that draft regulations must be issued for consultation with such organizations and persons that are likely to be affected. Section 51(6) provides similarly in relation to the issuance of guidance notes. FSA 2008 Section 44 provides that both the FSC and the Treasury must consult each other and any persons likely to be affected before issuing delegated legislation.

940. The Chief Secretary's Office issued a Code of Practice on Consultation in general (http://www.gov.im/lib/docs/cso/codeofpracticeonconsultation200.pdf). All new regulations and/or guidance notes are issued for full consultation and comments are invited from any interested parties. Responses are thoroughly reviewed and, where appropriate, changes are applied in a controlled and considered manner. The FSC publishes consultations and consultation feedback summaries on its website http://www.fsc.gov.im/doclibrary/condocs.xml.

941. Overall, therefore, the cooperation and coordination between the domestic authorities is well organized and effective. While the relative size of the Island's community facilitates this process, it may also increase the IOM's vulnerability to regulatory capture in the development and implementation of AML/CFT measures. The authorities validly place strong emphasis on inclusion of the financial sector in the development of pragmatic AML/CFT requirements and measures and it is important to balance this with the need to avoid compromising the effective implementation of measures that comply with the FATF Recommendations, for example, in the identification and verification of beneficial owner information.

6.1.2. Recommendations and Comments

none

6.1.3. Compliance with Recommendation 31

	Rating	Summary of factors underlying rating
R.31	**C**	

6.2. The Conventions and UN Special Resolutions (R.35 & SR.I)

6.2.1. Description and Analysis

Ratification of AML Related UN Conventions (c. 35.1):

942. As mentioned in section 1 of this report, the IOM is a British Crown Dependency and as such is not empowered to sign or ratify international conventions on its own behalf. Rather, the UK is

responsible for the IOM's international affairs and, following a request by the IOM Government, may extend the ratification of any convention to the IOM.

943. As a general principle, the IOM seeks to have extended to it all conventions ratified by the UK. However, such extension is only requested after IOM legislation has been determined to be in compliance with any given convention. Once that determination has been made and an extension has been requested, the UK Home Office reviews IOM legislation to confirm that it is in compliance with the provisions of the particular convention and advises the Ministry of Justice and the Foreign and Commonwealth Office accordingly. A notice is then sent to the Secretary-General of the United Nations, informing him that the ratification has been extended to the IOM. The same process is applied to international protocols.

944. Whereas the UK's ratification of the Vienna Convention has been extended to the IOM on December 2, 1993, extension of the Palermo Convention has not yet been requested as IOM law does not yet comply with all its provisions. At the time of the assessment there was no concrete timeframe for a request for extension of the Palermo Convention to the IOM.

Ratification of CFT Related UN Conventions (c. I.1):

945. The UK has extended ratification of the UN Convention for the Suppression of the Financing of Terrorism to the IOM on September 25, 2008.

946. Additionally, ten out of the other 15 international conventions and protocols relating to the fight against terrorism have been extended to IOM, namely the Diplomatic Agents Convention, the Civil Aviation Convention, the Maritime Convention, the Fixed Platforms Protocol, the Convention on the Making of Plastic Explosives for the Purpose of Detection, the Hostage Taking Convention, the Unlawful Seizure Convention, the Aircraft Convention, the Airport Protocol, and the Nuclear Material Convention.

Implementation of Vienna Convention (Articles 3-11, 15, 17 & 19, c. 35.1):

947. The IOM has implemented most of the Vienna Convention's provisions relevant to the FATF Recommendations. However, due to the common law principle of territoriality it appears that the IOM could not take jurisdiction over drug offenses or drug-based money laundering based only on the offenders' nationality or residency. Also, the confiscation provisions relating to proceeds derived from and instrumentalities of drug offenses fall short of the international standard as outlined in section 2 of this report.

Implementation of SFT Convention (Articles 2-18, c. 35.1 & c. I.1):

948. The IOM's legislation meets many of the requirements of the Suppression of the Financing of Terrorism Convention. However, as outlined in section 2 of this report, the terrorist financing offense does not fully meet the requirements of the international standard and shortcomings have also been identified with respect to the confiscation provisions relating to terrorist assets.

Implementation of Palermo Convention (Articles 5-7, 10-16, 18-20, 24-27, 29-31 & 34, c. 35.1):

949. The IOM has implemented some parts of the Palermo Convention's provisions relevant to the FATF Recommendations. However, further improvements in the laws will be required to fully implement all provisions of the Convention. In particular, self-laundering was not an offense at the time of the assessment for the acts of acquiring, possessing, or using criminal proceeds. Furthermore, the measures to confiscate proceeds of crime and instrumentalities used/intended for use in the crime are not fully in line with the international standard, as outlined under section 2 of this report.

Implementation of UNSCRs relating to Prevention and Suppression of FT (c. I.2)

950. As discussed under Special Recommendation III, the IOM's implementation of UNSCRs 1267 and 1373 seems to be largely sufficient.

Additional Element—Ratification or Implementation of Other relevant international conventions (c. 35.2):

951. In addition to the above referenced conventions and protocols, the UK's ratification of the 1990 Council of Europe Convention on Laundering, Search, Seizure, and Confiscation of the Proceeds from Crime has been extended to the IOM. While measures have been taken to bring IOM law in line with the provisions of the Merida Convention, at the time of the assessment, an extension of the UK's ratification to the IOM had not yet been requested.

6.2.2. Recommendations and Comments

- IOM should request extension to it of the Palermo Convention.
- The authorities should ensure that all provisions of the Palermo and Vienna Conventions are fully implemented.
- The authorities should ensure that all provisions of the United Nations International Convention for the Suppression of Financing of Terrorism are implemented.

6.2.3. Compliance with Recommendation 35 and Special Recommendation I

	Rating	Summary of factors underlying rating
R.35	**PC**	• Ratification of the Palermo Convention has not yet been extended to the IOM. • Not all provisions of the Palermo and Vienna Conventions are fully implemented.
SR.I	**PC**	• Not all provisions of the United Nations International Convention for the Suppression of Financing of Terrorism are implemented.

6.3. Mutual Legal Assistance (R.36-38, SR.V)

6.3.1. Description and Analysis

Legal Framework:

Domestic Legislation:

952. There is no overarching legislation regulating the mutual legal assistance (MLA) practice of the IOM. In providing such assistance, the judicial authorities use the domestic provisions contained in the CJA 1990, CJA 1991, DTA 1996, and ATCA 2003, as appropriate. In principle, all provisions apply to criminal activity both in and outside the IOM, except when expressly restricted to the IOM. As few of the provisions relating to the production of documents, searches, restraint, and confiscation are limited to criminal conduct or proceeds in the IOM, they can be directly applied to international requests for assistance.

953. Beside cooperation based on this general principle, there are also a number of bilateral mutual legal assistance treaties concluded by the UK that have been extended to the IOM:

i) Spain – Agreement between the UK and Spain concerning the prevention and suppression of drug trafficking and the misuse of drugs;

ii) Bahamas – Agreement between the UK and the Bahamas concerning the investigation of drug trafficking and confiscation of the proceeds of drug trafficking;

iii) Saudi Arabia – Agreement between the UK and Saudi Arabia concerning the investigation of drug trafficking and confiscation of the proceeds of drug trafficking;

iv) Sweden – Agreement between the UK and Sweden concerning the restraint and confiscation of proceeds of crime;

v) USA – Treaty between the UK and USA on Mutual Legal Assistance in Criminal Matters Treaty Series No.14 (1997); also Agreement between the UK and the USA on Investigation of Drug Trafficking Offenses and the Seizure and Forfeiture of the Proceeds of Drug Trafficking;

vi) Mexico – Agreement between the UK and Mexico concerning mutual assistance in relation to drug trafficking; also Agreement between the UK and Mexico on Mutual Assistance in the Investigation, Restraint and Confiscation of the Proceeds of Crime other than Drugs Trafficking;

vii) Ukraine – Agreement between the UK and the Ukraine concerning the Restraint and Confiscation of Proceeds and Instrumentalities of Criminal Activity other than Drug Trafficking Treaty Series No.47 (1997); also Agreement between the UK and the Ukraine on Mutual Assistance in Relation to Drug Trafficking;

viii) Thailand – Treaty between the UK and Thailand on Mutual Assistance in Criminal Matters; and

ix) Hong Kong – Agreement between the UK and Hong Kong concerning mutual assistance in criminal matters.

954. The 1959 European Convention on Mutual Legal Assistance also applies to the IOM under the umbrella of the UK. This instrument provides the main legal grounds for MLA requests to the jurisdictions that are party to this Convention.

Widest Possible Range of Mutual Assistance (c. 36.1):

955. The range of mutual legal assistance that can be provided according to the relevant Acts is quite broad and include following measures: collection, production, search, and seizure of information and documents.

956. In response to MLA requests in respect of suspected money laundering activity, the AG frequently uses the powers conferred to him by CJA 1990 Section 24, which provides for investigatory powers exercisable at the discretion of the AG where there is a suspected offense (wherever committed) involving 'serious or complex fraud'. Serious and complex fraud covers a wide range of criminal conduct, which is generally interpreted as all forms of dishonest behavior that produces illegal benefits. Under CJA 1990 Section 24 a person under investigation or any other person may be required to produce specified documents and if necessary provide an explanation of them. Section 24 also provides for a warrant to enter and search premises and seize documents. No court intervention is required, but the decisions of the AG may be made subject to judicial review to determine the 'reasonable' application of this provision.

957. In other circumstances evidence, witness statements, and search warrants can also be obtained according to Section 21 of the Criminal Justice Act 1991 ('the 1991 Act') providing for the AG to make an application to the High Bailiff to receive evidence. He must be satisfied that there are reasonable grounds to suspect that an offense has been committed and that an investigation or proceedings are in progress. This procedure is frequently applied in the judicial process of collecting evidence by taking witness statements under oath and to respond to an order or request to produce documents. The AG's discretion in making an application to the High Bailiff to receive evidence is subject to judicial review.

958. Section 22 of the 1991 Act provides for coercive measures of search and seizure in relation to material relevant to Section 21, to be obtained by making an application to a Deemster (i.e., a High Court judge). The Deemster must be satisfied that proceedings have been instituted or an arrest made, that the offense in the requesting country would constitute an 'arrestable' offense (as defined and listed in Section 27 of the PPPA 1998 and consequently including ML and FT) if it had occurred in the IOM and that there are reasonable grounds for suspecting that there is evidence on premises in the IOM which the suspect occupies or controls.

959. Requests in relation to drug offenses are dealt with according to the DTA 1996, Section 52 of which provides that for the purpose of a drug trafficking investigation a constable may make an application to a Deemster for an order for a person in possession of particular material to produce it to a constable for him to take it away or give access to it within a specified period, subject to certain conditions. Section 53 deals with applications for authority to search premises (Section 54 extends

‘premises’ to vehicles, vessels and aircraft, offshore installations, and tents or movable structures.). CJA 1990 Section 17J extends these provisions to any criminal proceeds investigation.

960. PPPA 1998 Sections 11 and 12 and Schedule 1 can also be invoked in MLA procedures, enabling a constable to obtain further production orders and search warrants. Section 11 empowers a Justice of the Peace to authorize the entry and search of premises on application by a constable when he is satisfied that there are reasonable grounds for believing that a serious ‘arrestable’ offense has been committed and there is material on the premises specified in the application which is likely to be of substantial value to the investigation (legal privilege, excluded material, or special procedure material excepted). Section 12 and Schedule 1 contain provisions allowing a constable on application to a Deemster to obtain access to excluded material (such as personal records and journalistic material), or special procedure (confidential) material under certain conditions.

961. Effecting service of judicial documents is adequately addressed in CJA 1990 Section 30. Facilitating the voluntary appearance of persons for the purpose of providing information or testimony to the requesting country does not require any specific legal provision, but is a normal form of assistance based on the goodwill of the AG and police.

962. As for confiscation of ML related assets and instrumentalities, see comments under Recommendation 38.

Provision of Assistance in Timely, Constructive and Effective Manner (c. 36.1.1):

963. Because of the developed offshore financial services industry of the IOM, MLA constitutes a substantial part of the workload of the judicial and law enforcement authorities. Rogatory commissions are dealt with in an organized manner aimed at an expeditious implementation, with two full-time Legal Officers (Financial Crime) in the AG’s Chambers handling and overseeing the incoming requests. There are no formal time frames for complying with such requests, but the following implementation procedure is applied in practice:

- acknowledgment of receipt of the request in two working days;

- a copy of the letter relating to financial offenses, such as ML and FT, is immediately sent to the FCU for preliminary investigations to establish the presence of relevant information;

- except for very complex requests, the aim is to execute the request and respond with the documents within three months.

No Unreasonable or Unduly Restrictive Conditions on Mutual Assistance (c. 36.2):

964. The IOM MLA policy is quite flexible and grounds for refusal are few. Each request is considered on its merits, but reciprocity is not a precondition nor is there a dual criminality reservation. Requests can be refused if these are considered to be politically motivated or when doubts arise on the due process and respect of basic human rights. Section 21 of the 1991 Act is the provision predominantly used to comply with requests for the production of evidence and witness statements and it only requires there are reasonable grounds to suspect that an offense under the law of the requesting country has been committed. It is not necessary that the conduct should constitute an

offense under the law of the IOM. Another condition is that criminal proceedings must have been instituted or a criminal investigation is ongoing in the requesting State.

965. The requirements for proceeding under CJA 1990 Section 24 are similar. There must be grounds to suspect serious or complex fraud (money laundering may fit in that concept) and it is sufficient that the request is made in the context of an investigation that has been initiated.

Efficiency of Processes (c. 36.3):

966. The procedure followed in implementing the requests is clear and simple as outlined above. The Legal Officers at the AG's Chambers review the letter of request to determine if the legal conditions are met and to decide on the appropriate method of execution. The request is acknowledged and a copy provided to the appropriate law enforcement unit, which would be the FCU if the request relates to proceeds of crime and FT. A team of three officers in the FCU deals with international assistance. A compliance or money laundering reporting officer is contacted at the institution concerned who then complies with the request under the appropriate procedure. If no court order is required, namely in cases of serious or complex fraud (CJA 1990 Section 24), a period of two or three weeks is the norm for complying with the request. For requests relating to other crimes and where witness statements are required, a court appearance is necessary (Section 21). Execution of rogatory letters according to this procedure takes longer, but the authorities endeavor to respond within a maximum of three months.

Provision of Assistance Regardless of Possible Involvement of Fiscal Matters (c. 36.4):

967. The fact that the request may contain fiscal aspects, both formally and in practice, does not constitute grounds for refusal. Even requests exclusively related to fiscal offenses are complied with under the conditions of Section 21 (3) of the 1991 Act, namely when proceedings have been instituted and if:

(a) the request emanates from a member of the Commonwealth or is made pursuant to a treaty to which the UK is a party and which extends to the IOM, or

(b) if the dual criminality criterion is fulfilled (mostly but not exclusively VAT and income tax).

Provision of Assistance Regardless of Existence of Secrecy and Confidentiality Laws (c. 36.5):

968. Provided that the requirements of Section 21 of the 1991 CJA or of Section 24 of CJA 1990 are met, the decision to grant assistance is at the discretion of the AG who does not consider himself constrained by secrecy or confidentiality considerations in meeting requests for assistance. If necessary, a court order would overrule any such obstacle, should it arise. The Banker's Books Evidence Act 1935 specifically provides for information in relation to banking records to be produced when ordered by a judge, confidentiality notwithstanding.

Availability of Powers of Competent Authorities (applying R.28, c. 36.6):

969. All law enforcement powers available domestically can equally be used in the context of international cooperation. More specifically production orders and search warrants can be obtained

pursuant to DTA 1996 Sections 52–54 (drug trafficking offenses) or to CJA 1990 Section 17J (other crimes). There is no legal requirement that the offenses must have taken place in the IOM.

Proceeds of Crime Act 2008:

970. Part 4 of the POCA 2008 contains provisions which duplicate and extend the provisions contained in the DTA 1996 and CJA 1990 with regard to production orders in relation to criminal confiscation investigations. The Act also contains additional powers providing for search and seizure warrants, disclosure orders, customer information orders, and account monitoring orders. POCA 2008 introduced a civil recovery procedure, which also provides for production orders and search warrants. The provisions of CJA 1990 Section 24 and the PPPA 1998 remain intact.

Avoiding Conflicts of Jurisdiction (c. 36.7):

971. There are no specific provisions in relation to conflict of jurisdiction, nor has any such difficulty presented itself in practice. This issue is normally dealt with on a case by case basis depending upon the circumstances and primarily where a prosecution is most likely to succeed.

Additional Element—Availability of Powers of Competent Authorities Required under R28 (c. 36.8):

972. No legislative provisions specifically prevent the use of the powers of competent authorities when a direct request is made by a foreign judicial or law enforcement authority to their IOM counterpart, but in practice the powers referred to above all require application to be made to court for an order and such applications are made by advocates from the AG's Chambers on behalf of the police. The AG is the central authority for the IOM and acts as the IOM counterpart for the foreign judicial authorities.

International Cooperation under SR V (applying c. 36.1-36.6 in R. 36, c. V.1):

973. The specific provisions referred to above in the DTA 1996 and CJA 1990 do not apply to terrorist offenses, but there are equivalent provisions in the ATCA 2003 (Sections 18, 24, and 25, and Schedules 4, 5, and 6). The law enforcement authorities are able to obtain documents and information for use in terrorist and terrorist financing investigations and prosecutions. This includes powers to use compulsory measures for the production of records held by financial institutions and other persons, for the search of persons and premises, and for the seizure and obtaining of evidence. Also the provisions of Section 21 and Schedule 2 of the Criminal Justice Act 1991 do not exclude terrorist offenses and can therefore be used to obtain depositions and evidence in respect of these offenses, including FT.

Dual Criminality and Mutual Assistance (c. 37.1 & 37.2):

974. As already stated, MLA in the form evidence gathering and witness statements does not require dual criminality. An exception applies in the case of fiscal offenses that could also have ML aspects, where proceedings have not been instituted and where the request is received from a country or territory which is a member of the Commonwealth or is made pursuant to a treaty to which the United Kingdom is a party and which extends to the IOM.

975. For restraint and confiscation orders, dual criminality is normally required. CJA 1990 Section 19 provides for the implementation of external confiscation orders for the purpose of recovering proceeds of criminal conduct 'corresponding to an offense to which this Part applies', meaning ML as criminalized by the Act in Sections 17A, B, and C. Although the IOM authorities do not require an identical formal qualification of the offense underlying the request and only consider the correspondence of the criminal conduct, difficulties could arise if the foreign request is based on the laundering of money generated by a predicate offense that is not covered under IOM law, as discussed under Recommendation 1.

International Cooperation under SR V (applying c. 37.1-37.2 in R. 37, c. V.2):

976. Requests related to terrorism matters, where the provisions of the ATCA 2003 have to be used, must meet a dual criminality standard to the extent that the purported criminal action must correspond with the definition of terrorism as defined in Section 29, which refers to the offenses considered to be of a terrorist nature under the Act. Consequently any deficiencies in the criminalization of FT may impact on the ability of the IOM to provide assistance if the request is based on activity that is not covered in IOM law.

Timeliness to Requests for Provisional Measures including Confiscation (c. 38.1):

977. In contrast to the flexibility of the MLA regime related to evidentiary matters, international cooperation requests for restraint, freezing, seizure, or confiscation are subject to more rigid conditions, as assistance can only be granted if the requesting country or territory is either the UK or a 'designated country or territory', as set out in secondary legislation.[70]

General regime

978. Foreign confiscation orders or decisions concerning non-drug and non-terrorism related offenses are dealt with in CJA 1990 Sections 18–22. Section 18 provides for the enforcement of UK confiscation orders, Section 19 for similar judicial decisions of other "designated" countries and jurisdictions. The designations are listed in Schedule 1 of the Criminal Justice Act 1990 (Designated Countries and Territories) Order 1996, supplemented by the Criminal Justice Act 1990 (Designated Countries and Territories) (Amendment) Orders of 1999, 2002, and 2003. In brief, foreign confiscation orders are executed as if they were domestic orders, with appointment of a receiver and realization of realizable property. The footnote outlines the amended provision going forward.

Drug Trafficking:

979. UK confiscation orders are enforceable in the IOM on the basis of DTA 1996 Section 35, in conjunction with the Drug Trafficking (Enforcement of United Kingdom Confiscation Orders) (Consolidation) Order 2004. Requests from other countries are governed by Section 36 of the Drug Trafficking Act 1996 together with the Drug Trafficking (Designated Countries and Territories)

[70] Subsequent to the assessment, this arrangement is due to change with the coming into force of POCA 2008 which introduces provisions that do not require 'designation' of relevant countries or territories from which requests may be considered.

Order 1999 providing for enforcement of confiscation orders made by designated countries and territories in the IOM, listed in Schedule 1 of the Order. The list of designated countries has since been amended and extended to other countries by Amendment Orders in 2002 and 2003. This legislation also provides for a receiver to be appointed and empowered to deal with property in the same manner as in the case of domestic trafficking. The footnote outlines the amended provision going forward.

980. Once approved by the AG, the same procedure is followed as for domestic confiscation orders, with the public prosecutor filing a request to the High Court to issue such order and, if necessary, appoint a receiver. Restraint orders can be issued in respect of any realizable property held by a specified person.

981. As for the confiscation of instrumentalities, which domestically falls under the application Section 16 of the CLA 1981 on the deprivation of the offender of property used or intended for use for the purpose of crime, there appears to be a lacuna as no allowances are made for external requests. Here the subject of the confiscation is the property or object itself, not a correspondent sum. The CJA 1990 provisions cannot be used either, as Section 19(2)(a)(i) restricts its application to 'property obtained as a result of or in connection with' criminal conduct.

Property of Corresponding Value (c. 38.2):

982. The implementation of foreign confiscation orders or decisions relating to corresponding value is no different from other criminal proceeds confiscations. The provisions of both the DTA 1996 and CJA 1990 require the court to determine the extent of benefit derived from the criminal conduct in order to issue a confiscation order for a specific sum which the defendant is required to satisfy. So in essence the confiscation orders relate to equivalent value anyway, not to a specific object or asset. If no voluntary payment follows, the court may, on application by the prosecutor, appoint and empower a receiver to realize the defendant's realizable property and apply the proceeds of that realization in satisfaction of the confiscation order.

Coordination of Seizure and Confiscation Actions (c. 38.3):

983. There are no formal arrangements for coordinating seizure and confiscation actions with other countries, but arrangements are made on a case-by-case basis with liaison between advocates of the AG's Chambers, officers of the FCU, and the requesting jurisdiction.

International Cooperation under SR V (applying c. 38.1-38.3 in R. 38, c. V.3):

984. Foreign requests for confiscation of funds used or to be used in the financing of terrorism are covered by the Anti-Terrorism (Enforcement of External Orders) Order 2004, enabling enforcement in the IOM of orders made by a court in a designated country or territory forfeiting terrorist property ('external orders'). The Order provides for the enforcement of such orders as if the order had originally been made by the High Court of the IOM as in ATCA 2003 Section 16. Designated countries and territories are specified in the Schedule to the Order. Schedule 2 of the Act provides further detail in respect of the implementation of forfeiture orders and provides for the appointment of a receiver to take possession of and realize any forfeited property.

985. Requests aiming at forfeiting the instrumentalities of TF crimes would meet with the same problem as outlined above.

986. As for the execution of foreign restraint orders, the Anti-Terrorism (Enforcement of External Orders) Order 2004 provides for that possibility when the request emanates from the appropriate authority of a designated country, aiming at restraining funds or other assets in the IOM on the grounds that they are terrorist property. In that case the Order requires that proceedings have been instituted and not yet concluded in the designated country, or application has been made to a court of the designated country for an external forfeiture order. The external restraint order is registered if the High Court is satisfied that, at the time of registration, the order is in force and the High Court is of the opinion that enforcing the order in the IOM would not be contrary to the interests of justice.

987. ATCA 2003 Section 16 relating to forfeiture in respect of a person convicted under any of Sections 7–10 of the Act, does not provide for equivalent value confiscation, but only for the forfeiture of money or other property when there is a direct or indirect link to the terrorism (funding) offenses under ATCA 2003 Section 7–10. Any requests to that end would face the same lacuna as outlined above under Recommendation 3.

Asset Forfeiture Fund (c. 38.4):

988. The IOM has established an asset forfeiture fund in respect of drug trafficking. Confiscated proceeds of drug trafficking are deposited in the fund and are used for law enforcement, health, education, and other appropriate purposes. Confiscated proceeds of other crimes are currently paid to the Treasury, but it is envisaged that a similar proceeds of crime fund will be established in respect of the proceeds of non-drug trafficking criminal conduct.

Sharing of Confiscated Assets (c. 38.5):

989. At the time of the on-site visit, there were no specific legislative provisions relating to the sharing of confiscated assets with other jurisdictions. Asset sharing was negotiated on a case-by-case basis. The POCA 2008 (from October 22, 2008) expressly provided for that possibility (Section 222(4)). A draft asset-sharing agreement is currently being negotiated between the IOM and the US and it is envisaged that further such agreements will be entered into once the Act is fully in force from August 1, 2009.

Additional Element (R 38) – Recognition of Foreign Orders for a) Confiscation of assets from organizations principally criminal in nature; b) Civil forfeiture; and, c) Confiscation of Property which Reverses Burden of Proof (applying c. 3.7 in R.3, c. 38.6):

990. Legislation currently in force in the IOM does not allow for confiscation without a conviction of any person (civil forfeiture), but this will be made possible by the civil recovery provisions in Part 1 of the POCA 2008. Once the necessary secondary legislation has been prepared, enforcement of foreign non-criminal confiscation orders will become effective.

Analysis:

991. MLA requests are frequently made to the IOM, which is to be expected considering the importance of the IOM as an offshore jurisdiction. The requests make up a substantial part of the

workload of the AG's office and the FCU, which are appropriately organized and resourced to deal with them. The overall picture is one of efficient assistance and constructive attitude. Generally, the legal conditions applied are consistent with the standard and the grounds for refusal are within accepted norms. In practice, there have been no refusals on record since 2004.

992. By contrast, the legal capability and decision-making scope of the IOM authorities to provide assistance requiring coercive conservatory or recovery measures is seriously restricted by the strict rule that only requests from designated countries can be considered. Each Act (CJA 1990, DTA 1996, and ATCA 2003) has its own list, there is no consolidated list and the last update occurred in 2003. Whatever the historical reason, this restriction is not in line with the international standards, not least as the law does not provide for any alternative means, such as the possibility of considering requests from non-designated jurisdictions on an ad hoc basis. The POCA 2008 (Sections 215 and 216, in force from August 1, 2009) should remedy this situation.

993. Some deficiencies of a technical/juridical nature may also affect the ability of the IOM to provide full assistance. The dual criminality principle, if strictly interpreted, may hamper the execution of foreign confiscation orders when based on predicates to ML or on FT activity that are not covered in the IOM criminal legislation. Furthermore, implementation of foreign confiscation orders related to equivalent value confiscation in terrorist financing cases and the forfeiture of instrumentalities generally may also meet with legal challenges.

Statistics (applying R.32):

994. The AG's Chambers keeps statistics on the number of cases where confiscated or restrained assets were repatriated (and at whose request), the number of confiscation orders made (all under the DTA 1996, the number of restraint orders and the requesting country. The number of rogatory letters received and from which country is also listed, as well as the legal grounds for the action taken. No statistical information was available on the amounts involved, nor the duration of the implementation process. No information was received on the number of requests made.

995. No requests related to FT have yet been received.

996. Overall, the IOM authorities take their responsibilities in respect of international cooperation seriously and adapt an overall constructive approach to all appropriate mutual legal assistance requests. Rigorously restricting such assistance in coercive matters to "designated countries" is however not acceptable under the international standards and any normative act in that sense should be abolished. The legal deficiencies in relation to the coverage of the ML and TF offenses (see R1 and SRII) spill over into the mutual legal assistance sphere where dual criminality is required, and should be addressed also in this context. Other issues to be (re)considered in the international cooperation area are the equivalent value confiscation in FT matters and the forfeiture of instrumentalities.

6.3.2. Recommendations and Comments

- Amend the law to correct the deficiencies affecting the criminalization of ML and FT offenses, and thus facilitate full compliance with MLA requests related to seizure and confiscation where the dual criminality principle applies.

- Remove the current restriction limiting MLA involving coercive conservatory and recovery matters to 'designated countries'.

- In amending the law in respect of the equivalent value confiscation and seizure in FT matters, remove also obstacles to related international mutual assistance.

6.3.3. Compliance with Recommendations 36 to 38 and Special Recommendation V

	Rating	Summary of factors relevant to s.6.3 underlying overall rating
R.36	**C**	
R.37	**C**	
R.38	**PC**	• Deficiencies in the ML criminalization affect the MLA capacity where the dual criminality principle applies. • Availability of MLA related to seizure and confiscation limited at time of assessment to 'designated' countries.
SR.V	**PC**	• Deficiencies in the FT criminalization affect the MLA capacity where the dual criminality principle applies. • Availability of MLA related to seizure and confiscation limited at time of assessment to 'designated' countries. • Equivalent value confiscation not provided for in FT matters, (also relevant in international cooperation context).

6.4. Extradition (R.37, 39, SR.V)

6.4.1. Description and Analysis

Legal Framework:

997. The extradition regime in the IOM is governed primarily by the UK Extradition Act of July 27, 1989. Section 29 of the Act provides that 'subject to the provisions of this section, Parts I to V of this Act extend to the Isle of Man, and have effect as if it were part of the United Kingdom.' Part III of the Act deals with extradition requests by foreign states to the UK (designated Commonwealth countries, States party to the European Convention on Extradition, States party to a bilateral treaty with the UK).

998. Also applicable since May 14, 1991 is the Council of Europe Convention on Extradition 1957, which according to its Article 27(2) considers the IOM to be included within the territorial application of the Convention to the UK. The Second additional Protocol (1978) to the Convention, related to fiscal offenses, was also extended to the IOM as of April 25, 2003. The IOM authorities would use this instrument whenever they address an outgoing extradition request to other countries party to the Convention. Incoming requests remain governed by the 1989 Extradition Act.

999. The European Arrest Warrant regime does not apply to the IOM, as it is not a member of the European Union.

1000. The IOM authorities informed the assessors that no extradition procedures have ever been initiated.

Dual Criminality and Mutual Assistance (c. 37.1 & 37.2):

1001. 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 Section 2 of the Extradition Act requiring the criminal conduct underlying the foreign extradition request also to be an offense in the UK, 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.

Money Laundering as Extraditable Offense (c. 39.1):

1002. Extraditable offenses ('extradition crime') are defined in Section 2 of the 1989 Extradition Act. Essentially they offenses relate to conduct in a foreign state which, if it occurred in the United Kingdom (for which read: the IOM), would constitute an offense punishable with imprisonment of 12 months and more and which is also so punishable under that law (subject to whatever qualification). Requests based on extraterritorial offenses are also complied with under certain conditions, though not of relevance in the context of this report.

1003. Offenses of concealing or transferring proceeds of drug trafficking, assisting another person to retain the benefit of drug trafficking and acquisition, possession or use of proceeds of drug trafficking under DTA 1996 Sections 45–47 are punishable upon conviction on information by imprisonment for a term not exceeding 14 years (or an unlimited fine or both). These money laundering and related offenses involving proceeds of drug trafficking are therefore extraditable offenses.

1004. The offense of assisting another to retain the benefit of criminal conduct under CJA 1990 Section 17A is punishable by custody up to 14 years (and/or an unlimited fine) and is therefore an extraditable offense. The same penalties apply to the acquisition, possession or use of proceeds of criminal conduct under Section 17B and concealing or transferring proceeds of criminal conduct under Section 17C. Consequently all these qualify as extraditable offenses.

1005. The terrorism related ML offense defined in ATCA 2003 Section 10 also qualifies, being punishable by custody of 14 years or more.

1006. The differentiation between drug related and other money laundering facts (except those related to terrorism) will disappear with the coming into force of the POCA 2008, with all of them potentially incurring a penalty of custody of more than 12 months (if tried on information). They consequently remain extraditable offenses.

Extradition of Nationals (c. 39.2):

1007. As in other common law jurisdictions, there is no legal obstacle to the IOM extraditing its own nationals.

Cooperation for Prosecution of Nationals (applying c. 39.2(b), c. 39.3):

1008. In the event of the IOM refusing to extradite, for whatever reason, the authorities indicated that they would then have recourse to Article 6(2) of the European Convention on Extradition, and endeavor to take over the prosecution from the requesting State. In that case the authorities would also coordinate with the requesting jurisdiction to ensure the efficiency of the prosecution (Article 12 of the Convention).

Efficiency of Extradition Process (c. 39.4):

1009. In dealing with an incoming extradition request the procedures outlined in Part III of the Extradition Act 1989 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. As there is no experience with such procedures in the IOM, there are no practical examples to be assessed in respect of efficiency and speed. In principle, the procedure provisions do not appear to contain unreasonable delay elements.

Extradition under SR V (applying c. 39.4 in R. 39, c V.4)

1010. FT is criminalized by ATCA Sections 7–10. These offenses 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 offenses within the scope of the Extradition Act 1989 and the Convention. Extradition based on such conduct follows the same principles and procedures as with those related to ML described above.

Additional Element under SR V (applying c. 39.5 in R. 39, c V.8)

1011. Section 14 of the Extradition Act provides for the possibility of simplified extradition procedures when the person who is the subject of the extradition request waives his rights.

Analysis:

1012. In the absence of precedents, only the formal provisions of the extradition regime can be assessed. The relevant legal framework is comprehensive and compliant with the international standards

1013. The dual criminality requirement, which in extradition matters is a broadly accepted, may in principle create problems in extradition requests related to ML or FT activity that is not formally covered under IOM criminal legislation. No case law is available to clarify this issue.

Statistics (applying R.32):

1014. There are no available statistics, in the absence of extraditions on record.

6.4.2. Recommendations and Comments

- Amend the law to correct the deficiencies affecting the criminalization of ML and FT offenses, and thus remove possible obstacles to complying with extradition requests where the dual criminality principle applies.

6.4.3. Compliance with Recommendations 37 & 39, and Special Recommendation V

	Rating	Summary of factors relevant to s.6.4 underlying overall rating
R.39	**LC**	• Deficiencies in the ML criminalization affect the extradition capacity where the dual criminality principle applies.
R.37	**C**	
SR.V	**PC**	• Deficiencies in the FT criminalization affect the extradition capacity where the dual criminality principle applies.

6.5. Other Forms of International Co-Operation (R.40 & SR.V)

6.5.1. Description and Analysis

Widest Range of International Cooperation (c. 40.1 and 40.2)

FIU

1015. Providing international cooperation to foreign counterparts is a very important part of the FIU assignment in an offshore jurisdiction like the IOM. The FCU/FIU is quite active in the Egmont network of FIUs over the Egmont Secure Web. Although not required, in some instances the cooperation is underpinned by bilateral MOUs. Information requests from a counterpart FIU are complied with to the greatest extent within the intelligence boundaries. The FIU to FIU cooperation is governed by the Egmont principles of information exchange ensuring that no further use of the information is made without the consent of the supplying FIU. The FCU normally grants its consent for intelligence purposes. Any other use would require a rogatory commission.

Customs

1016. The IOM Customs and Excise exchange information with their counterparts practically on a daily basis. The operational cooperation with the UK counterpart is well developed. The Customs and Excise Agreement with the UK and the Isle of Man Act 1979 and the Customs and Excise (Implementation of 1979 Agreement) Order 1980 provide for a free exchange of information with the UK Revenue and Customs relating to customs-specific matters, such as VAT, customs and excise duties, and related import/export issues. With the 1979 Agreement the IOM is also able to cooperate with EU Member States, as the Order applied the UK cooperation regime to the IOM. Customs and Excise also has arrangements under export control legislation for the exchange of information with the relevant bodies in the UK responsible for export licensing and controls.

1017. Being part of the customs territory of the EU, Customs and Excise 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.

Police

1018. Besides direct bilateral contacts, the police use the international communication network of Interpol. Assistance to other police authorities is routinely granted, as long as it does not involve coercive measures, such as taking voluntary witness statements and conducting informal enquiries. Such cooperation is done at intelligence level, and can, in principle, not be used in evidence without being confirmed in an MLA procedure.

Supervisory Authorities

1019. In relation to the powers of the FSC to exchange information, Schedule 5 to the FSA 2008 provides "gateways" which allow restricted information to be disclosed in certain circumstances. These circumstances include (amongst other gateways) disclosure -

(a) with a view to the institution of or otherwise for the purposes of criminal proceedings in the IOM or elsewhere;
(b) to a regulated authority, which is defined in FSA 2008 Section 48(1) as a governmental or private body in the IOM or elsewhere which has functions similar to those of the FSC; which regulates any profession; which regulates any financial services industry business or activities or any activities similar to a regulated activity; or which sets international standards for any financial services business; or

(c) to assist any authority in respect of law corresponding to the provisions of the Insider Dealing Act 1998; and in relation to functions corresponding to those of the IPA and of the FSC.

1020. In deciding whether to make a disclosure of customer information in line with (b) and (c) above, the FSC must consider a number of factors including the purpose for which the disclosure is required; whether the disclosure is appropriate with regard to its functions and regulatory objectives; whether the disclosure is likely to be of substantial value; whether the information could be obtained by other means; whether the body to which it is made is likely to keep the information confidential and secure; and whether the country concerned has reciprocal arrangements to disclose information to the IOM on request. These matters are purely for consideration and are not threshold tests. This consideration is not required for disclosures in line with (a) which is with a view to the institution of or otherwise for the purposes of criminal proceedings whether in the IOM or elsewhere.

1021. Pursuant to Schedule 5 of the Insurance Act 2008 (previously 22D of the Insurance Act 2004 as amended) the IPA has wide ranging powers to share information and to assist or enable another authority to undertake sharing of information, in particular to assist the counterparty to exercise its functions in relation to financial crime. (Schedule 5, Section 6(d)(3))

1022. Both the FSC and IPA are empowered (under the FSA 2008 and Insurance Act 2008, respectively) to enter into MOUs. As well as being a party to a number of bilateral MOUs, the FSC is

a full signatory to the IOSCO Multilateral Memorandum of Understanding (MMOU). The IPA is a signatory to a number of MOUs including agreements with counterparts in Hong Kong, Qatar and United Kingdom. The IPA has indicated its intention to enter into the multilateral memorandum of understanding currently under draft with the members of the International Association of Insurance Supervisors (IAIS).

Provision of Assistance in Timely, Constructive and Effective Manner (c. 40.1.1):

1023. All police and FIU ML/FT-related requests are handled by the FCU, more specifically by its international cooperation team. Requests are dealt with promptly in practice. No instances of undue delays have been signaled in the context of police and customs cooperation or as regards the supervisory authorities.

Spontaneous Exchange of Information (c. 40.3):

1024. The FCU/FIU has adopted a policy of informing the FIUs of the jurisdictions that are involved in an STR, whether or not requested to do so. The frequency of such spontaneous dissemination of information to counterpart FIUs is quite high, amounting to 635 cases in 2006, representing 38 percent of the total number of disclosures received by the FCU, and 343 cases in 2007 (22 percent of total).

1025. The Customs and Excise legal framework provides for both spontaneous and upon-request provision /exchange of information on ML and predicate offenses.

1026. Both the FSC and IPA are empowered to provide information to supervisory counterparties both spontaneously and on request. The scope of the powers includes all relevant information held by the supervisory authorities.

Making Inquiries on Behalf of Foreign Counterparts (c. 40.4): FIU Authorized to Make Inquiries on Behalf of Foreign Counterparts (c. 40.4.1):

1027. Police and Customs officers can use the powers available to them for domestic enquiries to obtain further information at the request of their foreign colleagues. The same applies to the FCU/FIU when collecting intelligence in ML/FT matters. Checking the own database and all other relevant sources accessible to the FCU is one part of the assistance provided.

1028. Under the FSA 2008, the FSA may use its powers of investigation in Schedule 2 on behalf of a regulatory authority with which it has entered into an MOU (and the Chief Executive is authorized to enter into such an agreement at his discretion). The powers in Schedule 2 include powers of inspection and investigation, powers to request and require information, and to apply for a search warrant where required. The FSC is also empowered under Schedule 3 of the Insider Dealing Act 1998 to undertake investigations on behalf of foreign authorities where there are grounds to suspect insider dealing. A similar range of powers is available to the IPA under the Insurance Act 2008, Schedule 5.

Conducting of Investigations on Behalf of Foreign Counterparts (c. 40.5):

1029. Interpol requests can be complied with as long as the investigation does not require invasive measures, so taking witness statements and collecting other information on a consensual basis presents no problem. Customs routinely conduct investigations in cross-border cases, such as VAT carousels and smuggling.

No Unreasonable or Unduly Restrictive Conditions on Exchange of Information (c. 40.6):

1030. For all law enforcement agencies the general rule is that, if the information is meant to be used as evidence by the requesting authority, this will have to be confirmed via a formal mutual assistance request. Otherwise no special conditions apply, except for the normal confidentiality and data protection rules.

1031. The FCU/FIU acts under the Egmont principles of information exchange, being the rule among all Egmont member FIUs. Information requests from other FIUs are considered on a case by case basis, but are usually complied with whenever the FCU is satisfied that the normal conditions will be observed.

1032. The matters where the supervisory authorities are to take into account in considering a request for information from a foreign counterpart were outlined earlier. While they would have the effect of preventing a 'fishing' expedition, they could not be considered unduly restrictive and appear to be applied flexibly in practice.

Provision of Assistance Regardless of Possible Involvement of Fiscal Matters (c. 40.7):

1033. Where a request might also relate to facts that have fiscal ramifications is in itself not grounds for refusal. If, however, the request relates exclusively to pure tax offenses, the approach is more cautious, though not prohibitive. For police cooperation it is important that the alleged facts can be translated into a criminal behavior recognized in IOM law (such as VAT carousels and false accounting). The FIU would in such case seek advice from the AG. Customs routinely cooperate directly in VAT carousel investigations.

Provision of Assistance Regardless of Existence of Secrecy and Confidentiality Laws (c. 40.8):

1034. Again, all depends if the request is done for evidentiary or for intelligence purposes. 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 mutual legal assistance basis. Such information can however also be shared without special formalities at police to police request for intelligence purposes, which is mostly done in preparation of a formal MLA request. The general rule applies that all information must be confirmed by way of rogatory commission if it is to be used in evidence.

1035. At FIU level the exchange of information takes place at intelligence level, irrespective of the nature of the counterpart FIU. Information of a more protected nature, such as financial and beneficial ownership data, can and is shared on an intelligence basis with foreign FIUs under the Egmont rules.

1036. There are no secrecy provisions in the IOM that would restrict the capacity of the supervisory authorities to share confidential information with foreign counterparts, where warranted and appropriate.

Safeguards in Use of Exchanged Information (c. 40.9):

1037. All relevant information, including requests for assistance and other information from foreign law enforcement sources, is stored in the secured central police database, to which the police and customs officers of the FCU have access. Use of the information is purpose bound under the Data Protection rules, namely for the prevention and detection of crime.

1038. Information supplied by counterpart FIUs is also registered in the police database, but access to it is restricted, with only the FCU/FIU department, the analysts, and the supervisors have full access to that part of the database. Moreover the Egmont rules imposing general confidentiality guarantees and prior consent conditions for the use of supplied information are observed.

1039. For the FSC, the statutory process of consideration of relevant factors that applies under the FSA 2008 for all information requests from counterparties provides an appropriate level of safeguards to protect confidential information from misuse. While these are matters that need to be taken into consideration, they do not automatically block the FSC from exchanging information where considered appropriate. Typically, information provided may not be passed to third parties without express FSC approval. A similar safeguard applies in respect of information provided to its counterparts by the IPA.

International Cooperation under SR V (applying c. 40.1-40.9 in R. 40, c. V.5):

1040. The direct cooperation regime between law enforcement authorities and FIUs equally applies in FT-related matters.

Analysis:

1041. The FCU, whether acting as an FIU or as an investigative body, maintains cooperative relationships with its counterparts. As the statistics show, the information exchanges are frequent (ranging between 89 and 149 per year in the last four years) and counterpart requests are responded to in a constructive way. Cooperation with other Egmont Group FIUs is actively conducted under the Egmont principles of information exchange providing for free exchange of information for analytical purposes and there are no refusals on record. The FCU follows a policy of flexibility when the requests can be handled in the intelligence stage, and consent to use the supplied information for intelligence purposes is not refused. Requests aimed at collecting evidence, however, need to follow the appropriate MLA procedures.

1042. The same constructive and effective approach to international cooperation is seen with the Customs and Excise, where exchanges of information and other forms of mutual assistance are an inherent part of their assignment.

Statistics (applying R.32)

1043. Detailed statistics on international requests for intelligence/assistance are kept by the FCU, including the number of spontaneous referrals. No distinction is made in the statistics, however, between police and FIU originated requests. It would give a clearer picture if the statistics would reflect that distinction.

1044. Statistics for various forms of international cooperation are also maintained by the supervisory authorities. Many of the information exchanges arise under the IOSCO MMOU, including those related to insider dealing. Information requests in conducting 'Fit and proper' tests represent another common application of international cooperation.

6.5.2. Recommendations and Comments

none

6.5.3. Compliance with Recommendation 40 and Special Recommendation V

	Rating	Summary of factors relative to s.6.5 underlying overall rating
R.40	**C**	
SR.V	**PC**	Deficiencies in the FT criminalization affect the extradition capacity where the dual criminality principle applies.

7. OTHER ISSUES

7.1. Resources and Statistics

1045. Factors and composite ratings for Recommendations 30 and 32 are as follows. The relevant analysis and recommendations may be found at appropriate points throughout the report.

	Rating	Summary of factors underlying rating
R.30	**LC**	• The regulatory authorities may require additional resources to sustain an appropriate level of AML/CFT onsite inspection work, particularly for banks and insurance businesses. • Some additional resources needed by the GSC and DHA.
R.32	**LC**	• Comprehensive statistics not maintained on seizures and confiscations.

7.2. Other relevant AML/CFT Measures or Issues

1046. There are no additional matters to raise.

7.3. General Framework for AML/CFT System (see also section 1.1)

1047. The general framework is addressed in section 1 of the report. No issues were identified that warrant further analysis.

Table 1. Ratings of Compliance with FATF Recommendations

Forty Recommendations	Rating	Summary of factors underlying rating[71]
Legal systems		
1. ML offense	**PC**	• Articles 17C CJA 1990 and 45 DTA 1996 are not sufficiently wide to fully meet the international standard due to the requirement that acts of "concealing or disguising" and "converting or transferring" are carried out with the purpose of avoiding prosecution for a predicate offense. • The defenses (payment of adequate consideration) provided for in Sections 17B (3) CJA 1990 and 47 (3) DTA 1996 are not provided for in the Vienna and Palermo Conventions and may allow money launderers to abuse the provision to avoid criminal liability for the acquisition, possession, or use of criminal proceeds. • Section 10 ATCA 2003 does not cover all material elements of the money laundering provisions of the Palermo and Vienna Conventions. • The offenses of acquisition, possession, or use in the CJA 1990 and the DTA 1996 as well as the money laundering offense contained in the ATCA 2003 do not extend to self-laundering. • The low level of relevant domestic investigations and prosecutions calls into question the effectiveness of the ML offense.
2. ML offense—mental element and corporate liability	**LC**	• While statutory sanctions for money laundering are comprehensive, dissuasive and proportional, the number of convictions obtained and the sentences actually imposed by the courts appear rather low. • It is difficult to assess the effectiveness of the stand-alone money laundering offense given that the provision has not yet been tested before the courts. The low number of investigations and prosecutions further supports the conclusion that money laundering is not yet dealt with as a stand-

[71] These factors are only required to be set out when the rating is less than Compliant.

		alone offense.
3. Confiscation and provisional measures	**PC**	• Deficiencies in ML and FT criminalization impact on the scope of criminal confiscation. • Confiscation of laundered assets might not succeed in stand-alone ML cases • At the time of the assessment, no equivalent value seizure possible before start of the proceedings. • For FT, barriers to application of equivalent value confiscation and seizure. • Overall effectiveness of confiscation measures needs to be improved.
Preventive measures		
4. Secrecy laws consistent with the Recommendations	**LC**	• Explicit exclusion from common law duty of client confidentiality not yet brought into force to permit financial institutions to exchange information.
5. Customer due diligence	**PC**	• Available concessions from conducting full CDD represent an overly-generous implementation of the FATF's facility to apply reduced or simplified measures for certain low-risk scenarios, including where the customer is acting on behalf of another person. Financial institutions not required in all cases to determine whether a customer is acting on behalf of another person and take reasonable steps to obtain sufficient identification data to verify the identity of that other person. • Current list of suggested high-risk customers omits some significant high risk business categories relevant in the IOM. • Some residual inconsistencies and potential overlap/conflict between pieces of AML/CFT secondary legislation. • Some exceptions to CDD requirements provided for only in guidance. • As they were recently introduced at the time of the on-site visit, the effectiveness of implementation of some CDD requirements, and of the supplementary provisions of the AML Code 2008, could be fully assessed.

6. Politically exposed persons	**C**	none
7. Correspondent banking	**C**	none
8. New technologies & non face-to-face business	**LC**	• Limited evidence of special attention to specific ML and FT risks of new technologies, including in relation to e-money and e-commerce and no evidence of testing by the FSC of implementation by financial institutions of appropriate measures. • As they were recently introduced at the time of the on-site visit, the effectiveness of implementation of the requirements regarding the risk of misuse of technologies and the risk resulting from non face-to-face business relationships could not be fully assessed.
9. Third parties and introducers	**LC**	• Not all permitted categories of introducer were subject to full AML/CFT requirements. • Indications of inconsistent implementation by financial institutions in relation to requirements in place at the time of on-site visit in applying due diligence relating to their reliance on Eligible Introducers, introducers, or Introducer's Certificates, as applicable
10. Record-keeping	**C**	none
11. Unusual transactions	**C**	none
12. DNFBP–R.5, 6, 8–11	**PC**	• Implementation arrangements for AML/CFT requirements were not yet in place for the accountancy profession. • In the case of CSPs and TSPs, the exceptions to the CDD requirements currently in the FSC Handbook lack a firm legal basis. • Effectiveness of implementation of the supplemental provisions of the AML Code 2008, other than for CSPs and TSPs, could not be assessed as they were adopted subsequent to the on-site visit.
13. Suspicious transaction reporting	**LC**	• Scope to improve timeliness of reporting of STRs to the FCU. • Comprehensive requirement needed to report attempted transactions that raise suspicions.
14. Protection & no tipping-off	**PC**	• The scope of the protection for STR reporting is not sufficient to include all categories of person or

		circumstances in the international standard and is not limited to good faith reporting.
15. Internal controls, compliance & audit	**LC**	• There is no requirement in law, regulation, or other enforceable means expressly covering AML/CFT to maintain an adequately resourced and independent audit function (having regard to the size and nature of the business).
16. DNFBP–R.13–15 & 21	**PC**	• No requirement to report attempted suspicious transactions. • Requirement for an independent audit function does not explicitly include AML/CFT within its scope. • Low levels of STR reporting by some categories of DNFBP. • Protection for those reporting suspicions not fully in line with international standard. • Effectiveness of implementation of the supplemental provisions of the AML Code 2008 could not be assessed as they were adopted subsequent to the on-site visit (other than CSPs and TSPs which were already subject to Part 9 of the FSC Rule Book from August 2008).
17. Sanctions	**LC**	• Limitation in the current scope of available administrative sanctions. • The effectiveness of the sanctions system is reduced by the low incidence of disciplinary measures applied by the FSC and the absence of any criminal prosecutions against persons contravening the AML/CFT requirements.
18. Shell banks	**C**	none
19. Other forms of reporting	**C**	none
20. Other NFBP & secure transaction techniques	**LC**	• Consideration not yet concluded on the application of AML/CFT requirements to other NFBPs
21. Special attention for higher risk countries	**LC**	• The process in place to ensure that financial institutions are advised of concerns about weaknesses in the AML/CFT systems of other countries had not been formalized at the time of the assessment.

22. Foreign branches & subsidiaries	**C**	none
23. Regulation, supervision and monitoring	**LC**	• Coverage of the AML/CFT requirements for financial institutions, though broad, is not fully comprehensive. • There is not yet in place an effective system of monitoring and ensuring compliance with AML/CFT requirements for money and value transfer service providers.
24. DNFBP—regulation, supervision and monitoring	**PC**	• Implementation of AML/CFT measures for DNFBPs, other than CSPs, TSPs, and most lawyers, is still being developed. • Registered legal practitioners are not adequately covered by the AML/CFT requirements. • The powers of the DHA to perform an AML/CFT supervisory role had not come into legal effect. • Additional supervisory resources needed for the DHA and GSC, including for the latter additional specialist skills to deal with on-line casino systems.
25. Guidelines & Feedback	**LC**	• Up-to-date guidance had not been issued by the GSC at the time of the assessment. • Guidance for accounting professionals not been adapted to the IOM requirements.
Institutional and other measures		
26. The FIU	**LC**	• No formal power of access to additional information for FIU analytical purposes. • Limited effectiveness of the overall reporting system, as reflected in low numbers of domestic FCU investigations.
27. Law enforcement authorities	**LC**	• Limited effectiveness of the system as reflected in low numbers of domestic investigations and prosecutions.
28. Powers of competent authorities	**C**	none
29. Supervisors	**LC**	• The supervisory authorities should, as planned, avail of their powers to conduct additional on-site inspections of banks and insurance businesses.
30. Resources, integrity, and training	**LC**	• The regulatory authorities may require additional resources to sustain an appropriate level of

		AML/CFT onsite inspection work, particularly for banks and insurance businesses. • Some additional resources needed by the GSC and DHA.
31. National co-operation	**C**	none
32. Statistics	**LC**	• Comprehensive statistics not maintained on seizures and confiscations.
33. Legal persons–beneficial owners	**LC**	• For about 30 percent of the 1931 Companies and LLCs, it could not be determined that accurate, complete, and current beneficial ownership information is available.
34. Legal arrangements – beneficial owners	**LC**	• 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.
International Cooperation		
35. Conventions	**PC**	• Ratification of the Palermo Convention has not yet been extended to the IOM. • Not all provisions of the Palermo and Vienna Conventions are fully implemented.
36. Mutual legal assistance (MLA)	**C**	none
37. Dual criminality	**C**	none
38. MLA on confiscation and freezing	**PC**	• Deficiencies in the ML criminalization affect the MLA capacity where the dual criminality principle applies. • Availability of MLA related to seizure and confiscation limited at time of assessment to 'designated' countries.
39. Extradition	**LC**	• Deficiencies in the ML criminalization affect the extradition capacity where the dual criminality principle applies
40. Other forms of co-operation	**C**	none
Nine Special Recommendations		
SR.I Implement UN instruments	**PC**	• Not all provisions of the United Nations International Convention for the Suppression of Financing of Terrorism are implemented.

SR.II	Criminalize terrorist financing	**LC**	• Article 1 ATCA 2003 does not contain a reference to international organizations. • The definition of "terrorism" in Section 1 ATCA 2003 does not extend to all terrorism offenses as defined in the nine Conventions and Protocols listed in the Annex to the FT Convention.
SR.III	Freeze and confiscate terrorist assets	**PC**	• No procedure in place to respond to and examine foreign freezing requests. • Definition of "funds" does not cover the 'jointly' and 'indirectly'. • No delisting or unfreezing procedure provided in the context of the EC Regulation lists. • No access provided to UNSCR 1267 frozen assets for humanitarian reasons and basic expenses.
SR.IV	Suspicious transaction reporting	**PC**	• The scope of the FT reporting requirement is limited by the incomplete coverage of ATCA 2003. • Scope to improve timeliness of reporting of STRs to the FCU. • Comprehensive requirement needed to report attempted transactions that raise suspicions.
SR.V	International cooperation	**PC**	• Deficiencies in the FT criminalization affect the capacity for MLA and extradition where the dual criminality principle applies. • Availability of MLA related to seizure and confiscation limited at time of assessment to 'designated' countries. • Equivalent value confiscation not provided for in FT matters, (also relevant in international cooperation context).
SR.VI	AML/CFT requirements for money/value transfer services	**LC**	• Active supervision for AML/CFT purposes of MVT providers had not commenced at the time of the assessment.
SR.VII	Wire transfer rules	**LC**	• Tighter implementation may be needed in applying the risk-based approach when dealing with wire transfers that lack full originator information.

		• Need for additional FSC monitoring of ongoing compliance with wire-transfer requirements
SR.VIII Nonprofit organizations	**LC**	• Review of NPO laws and regulations not yet complete. • Current coverage excludes NPOs that are outside the definition of charities.
SR.IX Cross-Border Declaration & Disclosure	**LC**	• The cross-border control regime does not cover cash transportation by mail between the UK and the IOM.

Table 2. Recommended Action Plan to Improve the AML/CFT System

FATF 40+9 Recommendations	Recommended Action (in order of priority within each section)
1. General	
2. Legal System and Related Institutional Measures	

2.1 Criminalization of Money Laundering (R.1 & 2)	• Amend Articles 17C CJA 1990 and 45 DTA 1996 to:
	  • provide for two alternative purposes for the acts of converting and transferring proceeds, namely to avoid prosecution for the predicate offense or to conceal the illicit origin of the funds, and;
	  • eliminate the purpose requirement for the acts of converting and transferring proceeds of crime.
	• The defense (payment of adequate consideration) provided for in Sections 17B(3) CJA 1990 and 47(3) DTA 1996 is not provided for in the Vienna and Palermo Conventions and should be eliminated as it may allow money launderers to abuse the provision to avoid criminal liability for the acquisition, possession, or use of criminal proceeds/proceeds.
	• Amend Section 10 ATCA 2003 to cover all material elements of the money laundering provisions of the Palermo and Vienna Conventions.
	• Amend the offenses of acquisition, possession, or use in the CJA 1990 and the DTA 1996 as well as the money laundering offense contained in the ATCA 2003 to include criminal proceeds obtained through the commission of a predicate offense by the self launderer.
	• The authorities should:
	(i) address any barriers to stand-alone ML prosecutions, including the level of proof needed to determine that property stems from the commission of a specific predicate offense; and
	(ii) take steps to develop jurisprudence on autonomous money laundering to establish that ML is a stand-alone offense.

2.2 Criminalization of Terrorist Financing (SR.II)	• Amend Article 1 ATCA 2003 to include a reference not only to governments but also to international organizations. • Amend the definition of "terrorism" in Section 1 ATCA 2003 to extend to all terrorism offenses as defined in the nine Conventions and Protocols listed in the Annex to the FT Convention.

	• Consider the impact of the including in the FT offense "intention of advancing a political, religious or ideological cause" on IOM's ability to successfully prosecute in factual settings contemplated by the FT Convention.
2.3 Confiscation, freezing, and seizing of proceeds of crime (R.3)	• The law should be amended to address the deficiencies affecting the scope of the ML and FT offenses and thereby also improve the quality of the criminal confiscation regime. • The law should be amended to: - allow equivalent value seizure at any stage of the investigation; and - address in ATCA 2003 the issue of equivalent value confiscation in the context of FT-related assets. • Case law should be developed on stand-alone money laundering confiscations. • The authorities should address the low effectiveness of the current asset recovery measures, particularly by focusing on the timely tracing and immobilization of recoverable or realizable assets.
2.4 Freezing of funds used for terrorist financing (SR.III)	• Put in place a formal procedure governing the receipt and assessment of requests based on foreign freezing lists, as required by UNSCR 1373. • Amend the legal framework implementing the UN Resolutions and EC Regulations to expressly extend the definition of 'funds' subject to freezing to cover assets 'jointly' or 'indirectly' owned or controlled by the relevant persons. • Amend the legal framework for the implementation of the EC Regulations to provide a procedure for considering requests for delisting or unfreezing. • Provide for and publicize a clear procedure enabling access to UNSCR 1267 frozen funds for humanitarian purposes and to cover basic expenses.
2.5 The Financial Intelligence Unit and its functions (R.26)	• The authorities should supplement the current informal arrangement by providing formally for access by the FIU to additional information held by covered entities, for use in its analytical work. • The FCU and other authorities should implement steps to improve the effectiveness of the reporting system to support an increase in the number of investigations and (potentially) prosecutions and in funds and other assets frozen.

2.6 Law enforcement, prosecution and other competent authorities (R.27 & 28)	• The authorities should implement steps to improve effectiveness by seeking to increase the number of investigations and prosecutions pursued domestically.
2.7 Cross-Border Declaration & Disclosure (SR IX)	• The cross-border control requirements should be extended to cover cash transportation by mail between the UK and the IOM.
3. Preventive Measures– Financial Institutions	
3.1 Risk of money laundering or terrorist financing	none
3.2 Customer due diligence, including enhanced or reduced measures (R.5–8)	**R.5** • The authorities should take steps to eliminate any residual inconsistencies in AML/CFT legal requirements and terminology. • The authorities should expand the current list of categories of higher-risk customers and consider including, for example, private banking and business involving trusts or other legal arrangements. • The authorities should conduct a risk-based review of the current scope of the Acceptable Applicant facility and, if warranted, limit its availability for consistency with the FATF Recommendations. To comply with the FATF Recommendations, financial institutions should be required in all cases to determine whether a customer is acting on behalf of another person and should take reasonable steps to obtain sufficient identification data to verify the identity of that other person. • If the exceptions to the CDD requirements of secondary legislation as currently set out in the FSC Handbook are to be retained, the authorities should amend the secondary legislation as necessary to provide for them. • Should the authorities decide to continue allowing source of funds to be used as principal evidence of identity in certain low-risk circumstances, the requirements should be tightened further to eliminate any remaining risk of abuse for ML or FT purposes. • The authorities should review on a risk basis the implementation of the concession allowing operations to commence prior to completion of full CDD procedures to ensure it is not being misused. • The authorities should ensure that insurance managers and insurance intermediaries are included within the scope of all

	relevant AML/CFT requirements. • The authorities should consider reducing significantly the current EUR15,000 threshold for the application of CDD measures to one-off transactions by MVT service providers. **R.8** • To support the implementation of the basic requirement in this area, the authorities should issue more detailed guidance on the specific ML and FT risks of new technologies, for example in relation to e-money and e-commerce.
3.3 Third parties and introduced business (R.9)	• The authorities should review the range of business introducers in respect of which concessions are applied to ensure that all categories are subject to equivalent AML/CFT requirements. • By means of on-site supervision or otherwise, the regulatory authorities should assess the effectiveness of CDD being obtained from Eligible Introducers or Introducers including, in the case of insurers, the use and effectiveness of Introducer's Certificates. • The authorities should remove any residual inconsistencies in secondary legislation following the coming into force of the AML Code 2008.
3.4 Financial institution secrecy or confidentiality (R.4)	• The authorities should bring into force the provision that financial institutions do not breach their confidentiality duty in exchanging customer information between themselves for AML/CFT purposes.
3.5 Record keeping and wire transfer rules (R.10 & SR.VII)	**SR.VII** • The FSC should reconsider whether the current implementation of the risk-based approach for incoming wire transfers lacking full originator information accurately reflect the level of underlying risk. • The FSC should continue to include wire transfers within its program of on-site supervision.
3.6 Monitoring of transactions and relationships (R.11 & 21)	• The authorities should formalize appropriate means of applying counter-measures to countries that do not or insufficiently apply the FATF Recommendations.
3.7 Suspicious transaction reports and other reporting (R.13, 14, 19, 25, & SR.IV)	**R.13** • The FCU and supervisory authorities should take steps to enhance the timeliness of reporting of suspicious transactions to the FCU.

	• The law should be amended to provide comprehensively that suspicious attempted transactions must be reported promptly to the FCU. **R.14** • The authorities should amend the law to extend the protection for persons reporting suspicions to the FIU to cover all aspects in the international standard and limit the protection to reporting in good faith. • The authorities should consider introducing measures to ensure the confidentiality, including in Court proceedings, of persons reporting suspicions to the FIU. **SR.IV** • The authorities should amend the law as needed to address the deficiencies in the scope of ATCA 2003 and thereby provide the required scope of coverage for STR reporting. • The FCU and supervisory authorities should take steps to enhance the timeliness of reporting of suspicious transactions to the FCU, including for suspicions of FT. • The law should be amended to provide comprehensively that suspicious attempted transactions must be reported promptly to the FCU.
3.8 Internal controls, compliance, audit and foreign branches (R.15 & 22)	• The authorities should supplement current provisions by introducing in law, regulation, or other enforceable means a requirement that, having regard to the size and nature of the business, financial institutions maintain an adequately resourced and independent audit function to test compliance with AML/CFT procedures.
3.9 Shell banks (R.18)	none
3.10 The supervisory and oversight system– competent authorities and SROs Role, functions, duties and powers (including sanctions) (R.23, 29, 17 & 25)	**R.17** • The FSC should consider issuing further regulations to allow it to impose additional administrative sanctions, where warranted. **R.23** • The authorities should apply AML and CFT requirements directly to any category of financial institutions not currently covered, having regard to such underlying ML and FT risks as may arise.

	• The FSC should proceed as planned to implement a supervisory regime for money-services businesses, including bureaux de change, as soon as possible. **R.29** • The FSC and IPA should make more frequent and extensive use of their powers to conduct AML/CFT on-site inspections of banks and insurance businesses, respectively.
3.11 Money value transfer services (SR.VI)	• The FSC should proceed at an early date to conduct AML/CFT supervision of MVT service providers. • The authorities should implement ongoing measures to identify any informal MVT service providers in the IOM. • The authorities should consider reducing significantly the current EUR15,000 threshold for the application of CDD measures to one-off transactions by MVT service providers.
4. Preventive Measures–Nonfinancial Businesses and Professions	
4.1 Customer due diligence and record-keeping (R.12)	• The authorities should keep under review the list of categories of higher-risk customers and consider including additional categories on a risk-related basis. • The authorities should conduct a risk-based review of the current scope of the Acceptable Applicant facility and, if warranted, limit its availability for consistency with the FATF Recommendations. • In the case of CSPs and TSPs, if the exceptions to the CDD requirements of secondary legislation as currently set out in the FSC Handbook are to be retained, the authorities should amend the secondary legislation as necessary to provide for them. • The authorities should review on a risk basis the implementation of the concession allowing operations to commence prior to completion of full CDD procedures to ensure it is not being misused, particularly in the case of advocates. • The DHA should proceed as quickly as possible with the planned arrangements to ensure that effective AML/CFT arrangements are place for accountancy professionals, including on a risk-sensitive basis those that are not members of either of the two main bodies. • The DHA should proceed as soon as possible with the planned

	implementation on a risk-sensitive basis of AML/CFT measures for dealers in high-value goods engaged in cash transactions. • The requirement to consider filing an STR if unable to adequately complete CDD measures should be extended to casinos.
4.2 Suspicious transaction reporting (R.16)	• Clarify the position of legal privilege in relation to ML and FT issues and STR reporting in a manner supportive of the AML/CFT system. • The authorities should continue their efforts, through awareness raising and otherwise, to increase the effectiveness of STR reporting by DNFBPs, particularly for those categories that rarely report suspicions. • The authorities should amend the law to extend the protection for persons reporting suspicions to the FIU to cover all aspects in the international standard and limit the protection to reporting in good faith. • The authorities should consider introducing measures to ensure the confidentiality, including in Court proceedings, of persons reporting suspicions to the FIU. • The authorities should introduce a requirement in law, regulation, or other enforceable means 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 authorities should amend the law to require the reporting of suspicious attempted transactions.
4.3 Regulation, supervision, monitoring, and sanctions (R.17, 24, & 25)	The authorities should: • Provide for and implement a system of regular and full audits for advocates based on onsite visits to monitor more closely the level of compliance with their AML/CFT obligations. • Ensure that registered legal practitioners are supervised to ensure their compliance with the provisions of the AML Code 2008. • Finalize the agreement between the DHA and the professional accounting bodies, issue guidance adapted to the IOM's AML/CFT requirements, and implement an AML/CFT on-site supervisory regime for the industry. • Formalize the basis for on-site assessments for DNFBPs that do not fall within the mandate of the FSC, GSC, or the IOM Law

	Society. • Proceed with planned legislative amendments to provide the DHA with adequate powers in undertaking registration and regulation for AML/CFT purposes of DNFBPs within its mandate and provide the DHA with resources consistent with that mandate. • Assess the adequacy of the GSC's staffing capacity and specialist skills base to ensure it is well positioned from an AML/CFT perspective to deal with the expected growth in on-line and terrestrial casino business.
4.4 Other designated non-financial businesses and professions (R.20)	• The authorities should proceed with their program of awareness-raising to determine what categories of NFBP should be within the scope of the AML/CFT requirements.
5. Legal Persons and Arrangements & Nonprofit Organizations	
5.1 Legal Persons–Access to beneficial ownership and control information (R.33)	• The authorities should seek to put in place measures to ensure that accurate, complete, and current beneficial ownership information is available for all 1931 Companies and LLCs. • The authorities should consider extending the formal monitoring of all corporate service providers for compliance with the requirements of the AML Code 2008 to include those "exempted" or "excluded" from the licensing requirements of the FSA 2008.
5.2 Legal Arrangements–Access to beneficial ownership and control information (R.34)	• The authorities should seek to put in place measures to ensure that accurate, complete and current beneficial ownership information is available for legal arrangements administered by a trustee who is not covered by the licensing requirements of FSA 2008. • The authorities should consider extending the formal monitoring of all trust service providers for compliance with the requirements of the AML Code 2008 to include those "exempted" or "excluded" from the licensing requirements of the FSA 2008.
5.3 Nonprofit organizations (SR.VIII)	• The authorities should complete the current review of the NPO laws and regulations and consider, based on an FT risk assessment, the merits of expanding the current coverage of charities to include other NPOs. • The authorities should conduct periodic vulnerability reviews

	and outreach to the NPO sector regarding the risk of abuse for FT purposes.
6. National and International Cooperation	
6.1 National cooperation and coordination (R.31)	none
6.2 The Conventions and UN Special Resolutions (R.35 & SR.I)	• IOM should request extension to it of the Palermo Convention. • The authorities should ensure that all provisions of the Palermo and Vienna Conventions are fully implemented. • The authorities should ensure that all provisions of the United Nations International Convention for the Suppression of Financing of Terrorism are implemented.
6.3 Mutual Legal Assistance (R.36, 37, 38 & SR.V)	• Amend the law to correct the deficiencies affecting the criminalization of ML and FT offenses, and thus facilitate full compliance with MLA requests related to seizure and confiscation where the dual criminality principle applies. • Remove the current restriction limiting MLA involving coercive conservatory and recovery matters to 'designated countries'. • In amending the law in respect of the equivalent value confiscation and seizure in FT matters, remove also obstacles to related international mutual assistance.
6.4 Extradition (R. 39, 37 & SR.V)	• Amend the law to correct the deficiencies affecting the criminalization of ML and FT offenses, and thus remove possible obstacles to complying with extradition requests where the dual criminality principle applies.
6.5 Other Forms of Cooperation (R. 40 & SR.V)	none
7. Other Issues	
7.1 Resources and statistics (R. 30 & 32)	**R.30** • Consideration should be given to assigning some additional resources to AML/CFT supervision of banks and insurance businesses, particularly to allow for an increase in on-site inspections. • Some additional resources needed by the GSC and DHA. The authorities should take steps to maintain comprehensive statistics on seizures and confiscations.

Annex 1. Authorities' Response to the Assessment

The Isle of Man authorities would like to thank the evaluators for the significant amount of time and resources which were devoted to preparing a comprehensive and constructive report. The discussions held as part of the evaluation allowed the assessors time also to understand how the different provisions are enforced, and this has contributed to a useful guide on how AML/CFT measures can continue to be improved.

The Island is fully committed to the Recommendations of the FATF on the prevention of money-laundering and the financing of terrorism. This commitment underpins the Island's regulatory regime and we believe has nurtured a culture of compliance throughout the jurisdiction.

When the Proceeds of Crime Act 2008 ("POCA 2008") came into operation on October 22, 2008, the report notes that not all of the legislation was brought into force at that time. POCA 2008 amalgamated drugs and all-crimes AML legislation and makes changes to the offences relating to Suspicious Transaction Reports. The remainder of the legislation has now come fully into force on August 1, 2009.

During 2009 a new Terrorism (Finance) Act 2009 completed its passage through Tynwald, and is now in force. This legislation provides Treasury with powers to issue directions to individuals or companies to enhance customer due diligence, monitoring or systematic reporting. It mirrors parts of the UK's Counter Terrorism Act which came into effect in November 2008. The Terrorism (Finance) Act 2009 allows the Island authorities to compile its own list of suspects subject to sanctions when required, such as if FATF advises measures against a country because of concerns regarding the financing of terrorism. It will also provide a new, local appeal mechanism for those subject to UN terrorism or Al-Qaida and the Taliban sanctions.

During 2009, work has been ongoing to develop an Anti-Terrorism and Crime (Amendment) Bill 2009 which is intended to further enhance the Island's counter terrorism legislation in line with developing international standards.

The Island's Criminal Justice (Money Laundering) Code 2008 will continue to be reviewed and revised where necessary.

The Island continues to place a very high priority on co-operation with regulators and law enforcement authorities in other jurisdictions, and in relation to taxation matters it continues to commit to Tax Information Exchange Agreements as it develops closer economic and taxation co-operation with other countries.

Annex 2. Details of All Bodies Met During the On-Site Visit

List of ministries, other government authorities or bodies, private sector representatives and others.

Lieutenant Governor of the Isle of Man
IOM Government (Treasury Minister, Chief Financial Officer, Chief Secretary)
Deemsters (Judges)
Attorney General's Chambers (AG)
Financial Supervision Commission (FSC) (including the Companies Registry)
Insurance and Pensions Authority (IPA)
Gambling Supervision Commission (GSC)
Financial Crime Unit (FCU)
Department of Home Affairs (DHA)
Customs & Excise
Office of Fair Trading (OFT)
General Registry

IOM Law Society
Institute of Chartered Accountants in England & Wales (ICAEW)
Association of Chartered Certified Accountants (ACCA)

Association of Licensed Banks (ALB)
Manx Insurance Association (MIA)
Manx Insurance Managers Association (MIMA)
Association of Corporate Service Providers (ACSP)
Fund Management Association (FMA)

5 individual banks
3 individual insurers
1 funds manager
1 securities firm
1 fiduciary
2 law firms
2 accountancy firms
2 bureau de change/payment system providers
1 real estate business
1 dealer in high value goods
1 casino
1 online gaming business

Annex 3. List of All Laws, Regulations, and Other Material Received

1. Criminal Justice Act 1990 (CJA 1990);
2. Criminal Justice Act 1991 (CJA 1991)
3. Drug Trafficking Act 1996 (DTA 1996);
4. Anti-Terrorism and Crime Act 2003 (ATCA 2003);
5. Anti-Terrorism (Enforcement of External Orders) Order 2004;
6. Criminal Law Act 1981;
7. Misuse of Drugs Act 1976;
8. Police Powers and Procedures Act 1998;
9. Regulation of Surveillance, Etc. Act 2006;
10. Al-Qa'ida and Taliban (United Nations Measures)(Isle of Man) Order 2002;
11. Terrorism (United Nations Measures)(Isle of Man) Order 2001;
12. Customs and Excise Management Act 1986;
13. European Communities (Wire Transfers Regulation) (Application) Order 2007;
14. European Communities (Wire Transfers Regulation) (Application) (Amendment) Order 2007;
15. The EC Wire Transfers Regulation (Enforcement) Regulations 2007;
16. Companies Act 2006;
17. Companies Act 1931-2004;
18. Extradition Act 1989;
19. Proceeds of Crime Act 2008 (POCA 2008);
20. Criminal Justice (Money Laundering) Code 2008 (Code 2008);
21. Anti-Money Laundering (Online Gambling and Peer to Peer Gambling) Code 2006;
22. Insider Dealing Act 1998;
23. Financial Services Act 2008 (FSA 2008);
24. FSC Financial Services Rule Book 2008 (part 9);

25. FSC AML/CFT Handbook 2008;

26. FSC General Licensing Policy;

27. Insurance Act 2008;

28. Insurance (Anti-Money Laundering) Regulations 2008 (IAMLR 2008);

29. Guidance Notes on Anti-Money Laundering and Preventing the Financing of Terrorism – for Insurers (Long Term Business) 2008 (IGN 2008)

30. Data Protection Act 2002;

31. Charities Acts 1962-1989.

Annex 4. Copies of Key Laws, Regulations, and Other Measures

The Annex contains:

1. Relevant extracts from:
    - Criminal Justice Act 1990 (CJA 1990);
    - Drug Trafficking Act 1996 (DTA 1996);
    - Anti-Terrorism and Crime Act 2003 (ATCA 2003);
    - Anti-Terrorism (Enforcement of External Orders) Order 2004;
    - Criminal Law Act 1981;
    - Misuse of Drugs Act 1976;
    - Al-Qa'ida and Taliban (United Nations Measures)(Isle of Man) Order 2002;
    - Terrorism (United Nations Measures)(Isle of Man) Order 2001;
    - Customs and Excise Management Act 1986;
    - Companies Act 2006;
    - Companies Act 1931-2004;
    - Extradition Act 1989.
2. Proceeds of Crime Act 2008 (POCA 2008) (index only).
3. Criminal Justice (Money Laundering) Code 2008 (Code 2008).
4. FSC Financial Services Rule Book 2008 (part 9).
5. Insurance (Anti-Money Laundering) Regulations 2008 (IAMLR 2008).

Criminal Justice Act (CJA) 1990

1 Confiscation orders

(1) The Court of General Gaol Delivery and any court of summary jurisdiction shall have power, in addition to dealing with an offender in any other way, to make an order under this section requiring him to pay such sum as the court thinks fit.

(2) The Court of General Gaol Delivery may make such an order against an offender where-

(a) he is found guilty of an offence to which this Part applies; and

(b) it is satisfied-

(i)that he has benefited from that offence or from that offence taken together with some other offence of which he is convicted in the same proceedings, or which the court takes into consideration in determining his sentence, and which is not a drug trafficking offence.

(ii) .....

(3) A court of summary jurisdiction may make such an order against an offender where-

(a) he is convicted of a prescribed offence; and

(b) it is satisfied-

(i)that he has benefited from that offence or from that offence taken together with some other prescribed offence of which he is convicted in the same proceedings, or which the court takes into consideration in determining his sentence.

(ii) .....

(4) For the purposes of this Part a person benefits from an offence if he obtains property as a result of or in connection with its commission and his benefit is the value of the property so obtained.

(5) Where a person derives a pecuniary advantage as a result of or in connection with the commission of an offence, he is to be treated for the purposes of this Part as if he had obtained as a result of or in connection with the commission of the offence a sum of money equal to the value of the pecuniary advantage.

(6) The sum which an order made by a court under this section requires an offender to pay shall be equal to-

(a) the benefit in respect of which it was made; or

(b) the amount appearing to the court to be the amount that might be realised at the time the order is made,

whichever is the less.

(7) .....

(7A) The standard of proof required to determine any question arising under this Part as to-

(a) whether a person has benefited from any offence;

(b) .....

(c) the amount to be recovered in his case under section 2,

shall be that applicable in civil proceedings.

(8) .....

(9) In this Part-

(a) an order made by the court under this section is referred to as a 'confiscation order';

(b) **'drug trafficking offence'** has the same meaning as in the Drug Trafficking Act 1996;

(c) references to an offence to which this Part applies are references to an offence which-

(i)is a prescribed offence; or

(ii)if not a prescribed offence, is an offence triable on information (whether or not it is exclusively so triable), other than a drug trafficking offence or an offence under any of sections 7 to 10 of the Anti-Terrorism and Crime Act 2003;

(d) a person against whom proceedings have been instituted for an offence to which this Part applies is referred to (whether or not he has been convicted) as the 'defendant';

(e) **'prescribed offence'** means an offence prescribed by order of the Department.

(10) An order under subsection (9)*(e)* shall be laid before Tynwald.

6 Cases in which restraint orders and charging orders may be made

(1) The powers conferred on the High Court by sections 7(l) and 8(l) are exercisable where-

(a) proceedings have been instituted in the Island against the defendant for an offence to which this Part applies;

(b) the proceedings have not been concluded; and

(c) either a confiscation order has been made or it appears to the court that there are reasonable grounds for thinking that a confiscation order may be made in them.

(2) Those powers are also exercisable where-

(a) the court is satisfied that, whether by the making of a complaint under section 4 of the Summary Jurisdiction Act 1989 or otherwise, a person is to be charged with an offence to which this Part applies; and

(b) it appears to the court that a confiscation order may be made in proceedings for the offence.

(3) For the purposes of sections 7 and 8 at any time when those powers are exercisable before proceedings have been instituted-

(a) references in this Part to the defendant shall be construed as references to the person referred to in subsection (2)*(a)*;

(b) references in this Part to the prosecutor shall be construed as references to the person who the High Court is satisfied is to have the conduct of the proposed proceedings; and

(c) references in this Part to realisable property shall be construed as if, immediately before that time, proceedings had been instituted against the person referred to in subsection (2)*(a)* for an offence to which

this Part applies.

(4) Where the court has made an order under section 7(l) or 8(l) by virtue of subsection (2), the court shall discharge the order if proceedings in respect of the offence are not instituted (whether by the making of a complaint under section 4 of the Summary Jurisdiction Act 1989 or otherwise) within such time as the court considers reasonable.

7 Restraint orders

(1) The High Court may by order (referred to in this Part as a 'restraint order') prohibit any person from dealing with any realisable property, subject to such conditions and exceptions as may be specified in the order.

(2) Without prejudice to the generality of subsection (1), a restraint order may make such provision as the court thinks fit for living expenses and legal expenses.

(3) A restraint order may apply-

(a) to all realisable property held by a specified person, whether the property is described in the order or not; and

(b) to realisable property held by a specified person, being property transferred to him after the making of the order.

(4) This section shall not have effect in relation to any property for the time being subject to a charge under section 8.

(5) A restraint order-

(a) may be made only on an application made by or with the consent of the Attorney General;

(b) may be made on an *ex parte* application to a Deemster in chambers; and

(c) shall provide for notice to be given to persons affected by the order.

(6) A restraint order-

(a) may be discharged or varied in relation to any property; and

(b) shall be discharged when proceedings for the offence are concluded.

(7) An application for the discharge or variation of a restraint order may be made by any person affected by it.

(8) Where the High Court has made a restraint order, the court may at any time appoint a receiver-

(a) to take possession of any realisable property, and

(b) in accordance with the court's directions, to manage or otherwise deal with any property in respect of which he is appointed,

subject to such exceptions and conditions as may be specified by the court; and may require any person having possession of property in respect of which a receiver is appointed under this section to give possession of it to the receiver.

(9) For the purposes of this section, dealing with property held by any person includes (without prejudice to the generality of the expression)-

(a) where a debt is owed to that person, making a payment to any person in reduction of the amount of the debt; and

(b) removing the property from the Island.

(10) Where the High Court has made a restraint order, a constable may for the purpose of preventing any realisable property being removed from the Island, seize the property.

(11) Property seized under subsection (10) shall be dealt with in accordance with the court's directions.

(12) The Land Registration Act 1982 shall apply-

(a) in relation to restraint orders, as it applies in relation to orders affecting land; and

(b) in relation to applications for restraint orders, as it applies in relation to other pending actions relating to land.

(13) The prosecutor shall be treated for the purposes of section 62 of the Land Registration Act 1982 (inhibitions) as a person interested in relation to any registered land to which the restraint order or an application for such an order relates.

17A Assisting another to retain the benefit of criminal conduct

(1) Subject to subsection (3), if a person enters into or is otherwise concerned in an arrangement whereby-

(a) the retention or control by or on behalf of another ('A') of A's proceeds of criminal conduct is facilitated (whether by concealment, removal from the jurisdiction, transfer to nominees or otherwise); or

(b) A's proceeds of criminal conduct-

(i)are used to secure that funds are placed at A's disposal; or

(ii)are used for A's benefit to acquire property by way of investment,

knowing or suspecting that A is a person who is or has been engaged in criminal conduct or has benefited from criminal conduct, he is guilty of an offence.

(2) In this section, references to any person's proceeds of criminal conduct include a reference to any property which in whole or in part directly or indirectly represented in his hands his proceeds of criminal conduct.

(3) Where a person discloses to a constable a suspicion or belief that any funds or investments are derived from or used in connection with criminal conduct or discloses to a constable any matter on which such a suspicion or belief is based-

(a) the disclosure shall not be treated as a breach of any restriction upon the disclosure of information imposed by statute or otherwise; and

(b) if he does any act in contravention of subsection (1) and the disclosure relates to the arrangement concerned, he does not commit an offence under this section if-

(i)the disclosure is made before he does the act concerned and the act is done with the consent of the constable; or

(ii)the disclosure is made after he does the act, but is made on his initiative and as soon as it is

reasonable for him to make it.

(4) In proceedings against a person for an offence under this section, it is a defence to prove-

(a) that he did not know or suspect that the arrangement related to any person's proceeds of criminal conduct; or

(b) that he did not know or suspect that by the arrangement-

(i)the retention or control by or on behalf of A of any property was facilitated; or

(ii)any property was used, as mentioned in subsection (1); or

(c) that-

(i)he intended to disclose to a constable such a suspicion, belief or matter as is mentioned in subsection (3) in relation to the arrangement; but

(ii)there is reasonable excuse for his failure to make disclosure in accordance with subsection (3)*(b)*.

(5) In the case of a person who was in employment at the relevant time, subsections (3) and (4) shall have effect in relation to disclosures, and intended disclosures, to the appropriate person in accordance with the procedure established by his employer for the making of such disclosures as they have effect in relation to disclosures, and intended disclosures, to a constable.

(6) A person guilty of an offence under this section shall be liable-

(a) on summary conviction, to custody for a term not exceeding 6 months or a fine not exceeding £5,000 or to both; or

(b) on conviction on information, to custody for a term not exceeding 14 years or a fine or to both.

(7) In this Part, **'criminal conduct'** means conduct which-

(a) constitutes an offence to which this Part applies; or

(b) would constitute such an offence if it had occurred in the Island.

17B Acquisition, possession or use of proceeds of criminal conduct

(1) A person is guilty of an offence if, knowing that any property is, or in whole or in part directly or indirectly represents, another person's proceeds of criminal conduct, he acquires or uses that property or has possession of it.

(2) It is a defence to a charge of committing an offence under this section that the person charged acquired or used the property or had possession of it for adequate consideration.

(3) For the purposes of subsection (2)-

(a) a person acquires property for inadequate consideration if the value of the consideration is significantly less than the value of the property; and

(b) a person uses or has possession of property for inadequate consideration if the value of the consideration is significantly less than the value of his use or possession of the property.

(4) The provision for any person of services or goods which are of assistance to him in criminal conduct shall not be treated as consideration for the purposes of subsection (2).

(5) Where a person discloses to a constable a suspicion or belief that any property is, or in whole or in part directly or indirectly represents, another person's proceeds of criminal conduct or discloses to a constable any matter on which such a suspicion or belief is based-

(a) the disclosure shall not be treated as a breach of any restriction upon the disclosure of information imposed by statute or otherwise; and

(b) if he does any act in relation to that property in contravention of subsection (1), he does not commit an offence under this section if-

(i)the disclosure is made before he does the act concerned and the act is done with the consent of the constable; or

(ii)the disclosure is made after he does the act, but is made on his initiative and as soon as it is reasonable for him to make it.

(6) For the purposes of this section, having possession of any property shall be taken to be doing an act in relation to it.

(7) In proceedings against a person for an offence under this section, it is a defence to prove that-

(a) he intended to disclose to a constable such a suspicion, belief or matter as is mentioned in subsection (5); but

(b) there is reasonable excuse for his failure to make the disclosure in accordance with subsection (5)*(b)*.

(8) In the case of a person who was in employment at the relevant time, subsections (5) and (7) shall have effect in relation to disclosures, and intended disclosures, to the appropriate person in accordance with the procedure established by his employer for the making of such disclosures as they have effect in relation to disclosures, and intended disclosures, to a constable.

(9) A person guilty of an offence under this section is liable-

(a) on summary conviction, to custody for a term not exceeding 6 months or a fine not exceeding £5,000 or to both; or

(b) on conviction on information, to custody for a term not exceeding 14 years or a fine or to both.

(10) No constable or other person shall be guilty of an offence under this section in respect of anything done by him in the course of acting in connection with the enforcement, or intended enforcement, of any provision of this Act or of any other enactment relating to criminal conduct or the proceeds of such conduct.

17C Concealing or transferring proceeds of criminal conduct

(1) A person is guilty of an offence if he-

(a) conceals or disguises any property which is, or in whole or in part directly or indirectly represents, his proceeds of criminal conduct; or

(b) converts or transfers that property or removes it from the jurisdiction,

for the purpose of avoiding prosecution for an offence to which this Part applies or the making or enforcement in his case of a confiscation order.

(2) A person is guilty of an offence if, knowing or having reasonable grounds to suspect that any property is, or in whole or in part directly or indirectly represents, another person's proceeds of criminal conduct, he-

(a) conceals or disguises that property; or

(b) converts or transfers that property or removes it from the jurisdiction,

for the purpose of assisting any person to avoid prosecution for an offence to which this Part applies or the making or enforcement in his case of a confiscation order.

(3) In subsections (1) and (2), the references to concealing or disguising any property include references to concealing or disguising its nature, source, location, disposition, movement or ownership or any rights with respect to it.

(4) A person guilty of an offence under this section is liable-

(a) on summary conviction, to custody for a term not exceeding 6 months or a fine not exceeding £5,000 or to both; or

(b) on conviction on information, to custody for a term not exceeding 14 years or a fine or to both.

18 Enforcement of United Kingdom orders

(1) The Department may by order provide that, for the purposes of sections 6 to 16, this Part shall have effect as if-

(a) references to confiscation orders included a reference to orders made (whether before or after the commencement of this Act) by courts in any part of the United Kingdom which appear to the Department to correspond to confiscation orders;

(b) references to proceedings in the Island or to the institution or conclusion in the Island of proceedings included a reference to proceedings in any part of the United Kingdom or to the institution or conclusion in any part of the United Kingdom of proceedings, as the case may be; and

(c) the references to the making of a complaint in section 6(2) and (4) included references to the laying of an information or the making of a complaint (as the case may be) under the corresponding legislation in the relevant part of the United Kingdom.

(2) An order under this section may provide for those sections to have effect in relation to anything done or to be done in any part of the United Kingdom subject to such further modifications as may be specified in the order.

(3) An order under this section may contain such incidental, consequential and transitional provisions as the Department considers expedient.

(4) An order under this section shall not come into operation until it is approved by Tynwald.

19 Enforcement of other external orders

(1) The Department may by order-

(a) direct in relation to a country or territory outside the Island and the United Kingdom designated by the order ('a designated country') that, subject to such modifications as may be specified, this Part shall apply to external confiscation orders and to proceedings which have been or are to be instituted in the designated country and may result in an external confiscation order being made there;

(b) make-

(i)such provision in connection with the taking of action in the designated country with a view to satisfying a confiscation order;

(ii)such provision as to evidence or proof of any matter for the purposes of this section and section 20; and

(iii)such incidental, consequential and transitional provision,

as appears to the Department to be expedient; and

(c) without prejudice to the generality of this subsection, direct that in such circumstances as may be specified proceeds which arise out of action taken in the designated country with a view to satisfying a confiscation order shall be treated as reducing the amount payable under the order to such extent as may be specified.

(2) In this Part-

'external confiscation order' means an order made (whether before or after the commencement of this Part) by a court in a designated country for the purpose-

(a) of recovering-

(i) property obtained as a result of or in connection with conduct corresponding to an offence to which this Part applies; or

(ii) the value of the property so obtained; or

(b) of depriving a person of a pecuniary advantage so obtained; and

'modifications' includes additions, alterations and omissions.

(3) The power to make an order under this section includes power to modify this Part in such a way as to confer power on a person to exercise a discretion.

(4) An order under this section shall not come into operation until it is approved by Tynwald.

20 Registration of external confiscation orders

(1) On an application made by or on behalf of the Government of a designated country, the High Court may register an external confiscation order made there if-

(a) it is satisfied that at the time of registration the order is in force and not subject to appeal;

(b) it is satisfied, where the person against whom the order is made did not appear in the proceedings, that he received notice of the proceedings in sufficient time to enable him to defend them; and

(c) it is of the opinion that enforcing the order in the Island would not be contrary to the interests of justice.

(2) In subsection (1), 'appeal' includes-

(a) any proceedings by way of discharging or setting aside a judgment; and

(b) an application for a new trial or a stay of execution.

(3) The High Court shall cancel the registration of an external confiscation order if it appears to the court that the order has been satisfied by the payment of the amount due under it or by the person against whom it was made serving imprisonment in default of payment or by any other means.

21 Disclosure of information subject to statutory or other restriction on disclosure

Where a person discloses to a constable-

(a) a suspicion or belief that any property-

(i)has been obtained as a result of or in connection with the commission of an offence to which this Part applies or conduct corresponding to such an offence; or

(ii)derives from property so obtained; or

(b) any matter on which such a suspicion or belief is based,

the disclosure shall not be treated as a breach of any restriction upon the disclosure of information imposed by statute or otherwise.

Drug Trafficking Act (DTA) 1996

2 Confiscation orders

(1) Where a defendant appears before the Court of General Gaol Delivery to be sentenced in respect of one or more drug trafficking offences (and has not previously been sentenced or otherwise dealt with in respect of his conviction for the offence or, as the case may be, any of the offences concerned), then-

(a) if the prosecutor asks the court to proceed under this section, or

(b) if the court considers that, even though the prosecutor has not asked it to do so, it is appropriate for it to proceed under this section,

it shall act as follows.

(2) The court shall first determine whether the defendant has benefited from drug trafficking.

(3) For the purposes of this Act, a person has benefited from drug trafficking if he has at any time (whether before or after the commencement of this Act) received any payment or other reward in connection with drug trafficking carried on by him or another person.

(4) If the court determines that the defendant has so benefited, the court shall, before sentencing or otherwise dealing with him in respect of the offence or, as the case may be, any of the offences concerned, determine in accordance with section 5 the amount to be recovered in his case by virtue of this section.

(5) The court shall then, in respect of the offence or offences concerned-

(a) order the defendant to pay that amount;

(b) take account of the order before-

(i) imposing any fine on him;

(ii) making any order involving any payment by him; or

(iii) making any order under section 27 of the Misuse of Drugs Act 1976 (forfeiture orders) or

section 16 of the Criminal Law Act 1981 (deprivation orders); and

(c) subject to paragraph *(b)*, leave the order out of account in determining the appropriate sentence or other manner of dealing with him.

(6) No enactment restricting the power of a court dealing with an offender in a particular way from dealing with him also in any other way shall by reason only of the making of an order under this section restrict the Court of General Gaol Delivery from dealing with an offender in any way the court considers appropriate in respect of a drug trafficking offence.

(7) The standard of proof required to determine any question arising under this Act as to-

(a) whether a person has benefited from drug trafficking, or

(b) the amount to be recovered in his case by virtue of this section,

shall be that applicable in civil proceedings.

(8) In this Act **'confiscation order'** means an order under this section and includes, in particular, such an order made by virtue of section 13, 14 or 19.

25 Cases in which restraint orders and charging orders may be made

(1) The powers conferred on the High Court by sections 26(1) and 27(1) are exercisable where-

(a) proceedings have been instituted in the Island against the defendant for a drug trafficking offence or an application has been made by the prosecutor in respect of the defendant under section 13, 14, 15, 16 or 19;

(b) the proceedings have not, or the application has not, been concluded; and

(c) the court is satisfied that there is reasonable cause to believe-

(i) in the case of an application under section 15 or 16, that the court will be satisfied as mentioned in section 15(4) or, as the case may be, 16(2); or

(ii) in any other case, that the defendant has benefited from drug trafficking.

(2) The court shall not exercise those powers by virtue of subsection (1) if it is satisfied-

(a) that there has been undue delay in continuing the proceedings or application in question; or

(b) that the prosecutor does not intend to proceed.

(3) The powers mentioned in subsection (1) are also exercisable where-

(a) the court is satisfied that, whether by the making of a complaint or otherwise, a person is to be charged with a drug trafficking offence or that an application of a kind mentioned in subsection (1)*(a)* is to be made in respect of the defendant;

(b) the court is also satisfied as mentioned in subsection (1)*(c)*.

(4) For the purpose of sections 26 and 27, at any time when those powers are exercisable before proceedings have been instituted-

(a) references in this Act to the defendant shall be construed as references to the person referred to in subsection (3)*(a)*;

(b) references in this Act to the prosecutor shall be construed as references to the person who the High Court is satisfied is to have the conduct of the proposed proceedings; and

(c) references in this Act to realisable property shall be construed as if, immediately before that time, proceedings had been instituted against the person referred to in subsection (3)*(a)* for a drug trafficking offence.

(5) Where the court has made an order under section 26(1) or 27(1) by virtue of subsection (3), the court shall discharge the order if proceedings in respect of the offence are not instituted, whether by the making of a complaint or otherwise, or (as the case may be) if the application is not made, within such time as the court considers reasonable.

26 Restraint orders

(1) The High Court may by order (in this Act referred to as a **'restraint order'**) prohibit any person from dealing with any realisable property, subject to such conditions and exceptions as may be specified in the order.

(2) A restraint order may apply-

(a) to all realisable property held by a specified person, whether the property is described in the order or not; and

(b) to realisable property held by a specified person, being property transferred to him after the making of the order.

(3) This section shall not have effect in relation to any property for the time being subject to a charge under section 27 of this Act or section 9 of the Drug Trafficking Offences Act 1987.

(4) A restraint order-

(a) may be made only on an application by the prosecutor;

(b) may be made on an ex parte application to a Deemster in chambers; and

(c) shall provide for notice to be given to persons affected by the order.

(5) A restraint order-

(a) may be discharged or varied in relation to any property; and

(b) shall be discharged on the conclusion of the proceedings or of the application in question.

(6) Where the High Court has made a restraint order, the High Court-

(a) may at any time appoint a receiver-

(i) to take possession of any realisable property, and

(ii) in accordance with the court's directions, to manage or otherwise deal with any property in respect of which he is appointed,

subject to such exceptions and conditions as may be specified by the court; and

(b) may require any person having possession of property in respect of which a receiver is appointed under this section to give possession of it to the receiver.

(7) For the purposes of this section, dealing with property held by any person includes (without prejudice to the generality of that expression)-

(a) where a debt is owed to that person, making a payment to any person in reduction of the amount of the debt; and

(b) removing the property from the Island.

(8) Where a restraint order has been made a constable may seize any realisable property for the purpose of preventing its removal from the Island.

(9) Property seized under subsection (8) shall be dealt with in accordance with the directions of the court.

(10) An application for the discharge or variation of a restraint order may be made by any person affected by it.

(11) The Land Registration Act 1982 shall apply-

(a) in relation to restraint orders, as it applies in relation to orders affecting land; and

(b) in relation to applications for restraint orders, as it applies in relation to other pending actions relating to land.

(12) The prosecutor shall be treated for the purposes of section 62 of the Land Registration Act 1982 (inhibitions) as a person interested in relation to any registered land to which a restraint order or an application for such an order relates..

35 Enforcement of United Kingdom orders

(1) The Department may by order provide that, for the purposes of sections 17 and 25 to 34, this Act shall have effect as if-

(a) references to confiscation orders included a reference to orders made (whether before or after the commencement of this Act) by courts in any part of the United Kingdom which appear to the Department to correspond to confiscation orders;

(b) references to drug trafficking offences included a reference to any offence under the law of any part of the United Kingdom which appears to the Department to correspond to a drug trafficking offence;

(c) references to proceedings in the Island or to the institution or conclusion in the Island of proceedings included a reference to proceedings in any part of the United Kingdom or to the institution or conclusion in any part of the United Kingdom of proceedings, as the case may be; and

(d) the references to the making of a complaint in section 25(3) and (5) included references to laying an information or making a complaint (as the case may be) under the corresponding law in the relevant part of the United Kingdom.

(2) An order under this section may provide for those sections to have effect, in relation to anything done or to be done in any part of the United Kingdom, subject to such further modifications as may be specified in the order.

(3) An order under this section may contain such incidental, consequential and transitional provisions as the Department considers expedient.

(4) An order under this section shall not come into operation unless it is approved by Tynwald.

36 Enforcement of external confiscation orders

(1) The Department may by order-

(a) direct in relation to a country or territory outside the Island and the United Kingdom designated by the order ('a designated country') that, subject to such exceptions, adoptions and modifications as may be specified, this Act shall apply to external confiscation orders and to proceedings which have been or are to be instituted in the designated country and may result in an external confiscation order being made there;

(b) make-

(i)such provision in connection with the taking of action in the designated country with a view to satisfying a confiscation order,

(ii)such provision as to evidence or proof of any matter for the purposes of this section and section 37, and

(iii)such incidental, consequential and transitional provisions,

as appears to the Department to be expedient; and

(c) without prejudice to the generality of this subsection, direct that, in such circumstances as may be specified, proceeds which arise out of action taken in the designated country with a view to satisfying a confiscation order shall be treated as reducing the amount payable under the order to such extent as may be specified.

(2) In this section, 'external confiscation order' means an order made by a court in a designated country for the purpose of recovering, or recovering the value of, payments or other rewards received in connection with drug trafficking.

(3) The power to make an order under this section includes power to modify the relevant provisions of this Act in such a way as to confer power on a person to exercise a discretion.

(4) An order under this section shall not come into operation unless it is approved by Tynwald.

(5) An order under this section may make a direction to apply-

(a) generally in respect of all countries and territories;

(b) in respect of specified countries and territories; or

(c) in respect of classes of countries and territories,

and reference to a 'designated country' shall be construed accordingly.

37 Registration of external confiscation orders

(1) On an application made by or on behalf of the Government of a designated country, the High Court may register an external confiscation order made there if-

(a) it is satisfied that at the time of registration the order is in force and not subject to appeal;

(b) it is satisfied, where the person against whom the order is made did not appear in the proceedings, that he received notice of the proceedings in sufficient time to enable him to defend them; and

(c) it is of the opinion that enforcing the order in the Island would not be contrary to the interests of

justice.

(2) In subsection (1), 'appeal' includes-

(a) any proceedings by way of discharging or setting aside a judgment; and

(b) an application for a new trial or a stay of execution.

(3) The High Court shall cancel the registration of an external confiscation order if it appears to the court that the order has been satisfied by payment of the amount due under it.

(4) In this section 'designated country' and 'external confiscation order' have the same meaning as in section 36.

45 Concealing or transferring proceeds of drug trafficking

(1) A person is guilty of an offence if he-

(a) conceals or disguises any property which is, or in whole or in part directly or indirectly represents, his proceeds of drug trafficking, or

(b) converts or transfers that property or removes it from the jurisdiction,

for the purpose of avoiding prosecution for a drug trafficking offence or the making or enforcement in his case of a confiscation order.

(2) A person is guilty of an offence if, knowing or having reasonable grounds to suspect that any property is, or in whole or in part directly or indirectly represents, another person's proceeds of drug trafficking, he-

(a) conceals or disguises that property, or

(b) converts or transfers that property or removes it from the jurisdiction,

for the purpose of assisting any person to avoid prosecution for a drug trafficking offence or the making or enforcement of a confiscation order.

(3) In subsections (1)*(a)* and (2)*(a)* the references to concealing or disguising any property include references to concealing or disguising its nature, source, location, disposition, movement or ownership or any rights with respect to it.

46 Assisting another person to retain the benefit of drug trafficking

(1) Subject to subsection (3), a person is guilty of an offence if he enters into or is otherwise concerned in an arrangement whereby-

(a) the retention or control by or on behalf of another person (call him 'A') of A's proceeds of drug trafficking is facilitated (whether by concealment, removal from the jurisdiction, transfer to nominees or otherwise), or

(b) A's proceeds of drug trafficking-

(i) are used to secure that funds are placed at A's disposal, or

(ii) are used for A's benefit to acquire property by way of investment,

and he knows or suspects that A is a person who carries on or has carried on drug trafficking or has benefited from drug trafficking.

(2) In this section, references to any person's proceeds of drug trafficking include a reference to any property which in whole or in part directly or indirectly represented in his hands his proceeds of drug trafficking.

(3) Where a person discloses to a constable a suspicion or belief that any funds or investments are derived from or used in connection with drug trafficking, or discloses to a constable any matter on which such a suspicion or belief is based-

(a) the disclosure shall not be treated as a breach of any restriction upon the disclosure of information imposed by statute or otherwise, and

(b) if he does any act in contravention of subsection (1) and the disclosure relates to the arrangement concerned, he does not commit an offence under this section if-

(i) the disclosure is made before he does the act concerned and the act is done with the consent of the constable; or

(ii) the disclosure is made after he does the act, but is made on his initiative and as soon as it is reasonable for him to make it.

(4) In proceedings against a person for an offence under this section, it is a defence to prove-

(a) that he did not know or suspect that the arrangement related to any person's proceeds of drug trafficking;

(b) that he did not know or suspect that by the arrangement the retention or control by or on behalf of A of any property was facilitated or, as the case may be, that by the arrangement any property was used as mentioned in subsection (1)*(b)*; or

(c) that-

(i) he intended to disclose to a constable such a suspicion, belief or matter as is mentioned in subsection (3) in relation to the arrangement, but

(ii) there is reasonable excuse for his failure to make any such disclosure in the manner mentioned in subsection (3)*(b)*.

(5) In the case of a person who was in employment at the time in question, subsections (3) and (4) shall have effect in relation to disclosures, and intended disclosures, to his employer or, where his employer has established a procedure for the making of such disclosures, to the appropriate person in accordance with the procedure, as they have effect in relation to disclosures, and intended disclosures, to a constable.

47 Acquisition, possession or use of proceeds of drug trafficking

(1) A person is guilty of an offence if, knowing that any property is, or in whole or in part directly or indirectly represents, another person's proceeds of drug trafficking, he acquires or uses that property or has possession of it.

(2) It is a defence to a charge of committing an offence under this section that the person charged acquired or used the property or had possession of it for adequate consideration.

(3) For the purposes of subsection (2)-

(a) a person acquires property for inadequate consideration if the value of the consideration is

significantly less than the value of the property; and

(b) a person uses or has possession of property for inadequate consideration if the value of the consideration is significantly less than the value of his use or possession of the property.

(4) The provision for any person of services or goods which are of assistance to him in drug trafficking shall not be treated as consideration for the purposes of subsection (2).

(5) Where a person discloses to a constable a suspicion or belief that any property is, or in whole or in part directly or indirectly represents, another person's proceeds of drug trafficking, or discloses to a constable any matter on which such a suspicion or belief is based-

(a) the disclosure shall not be treated as a breach of any restriction upon the disclosure of information imposed by statute or otherwise; and

(b) if he does any act in relation to the property in contravention of subsection (1), he does not commit an offence under this section if-

(i) the disclosure is made before he does the act concerned and the act is done with the consent of the constable; or

(ii) the disclosure is made after he does the act, but is made on his initiative and as soon as it is reasonable for him to make it.

(6) For the purposes of this section, having possession of any property shall be taken to be doing an act in relation to it.

(7) In proceedings against a person for an offence under this section, it is a defence to prove that-

(a) he intended to disclose to a constable such a suspicion, belief or matter as is mentioned in subsection (5), but

(b) there is reasonable excuse for his failure to make any such disclosure in the manner mentioned in subsection (5)*(b)*.

(8) In the case of a person who was in employment at the time in question, subsections (5) and (7) shall have effect in relation to disclosures, and intended disclosures, to his employer or, where his employer has established a procedure for the making of such disclosures, to the appropriate person in accordance with the procedure, as they have effect in relation to disclosures, and intended disclosures, to a constable.

(9) No constable or other person shall be guilty of an offence under this section in respect of anything done by him in the course of acting in connection with the enforcement, or intended enforcement, of any provision of this Act or of any other enactment relating to drug trafficking or the proceeds of drug trafficking.

48 Failure to disclose knowledge or suspicion of money laundering

(1) A person is guilty of an offence if-

(a) he knows or suspects that another person is engaged in drug money laundering,

(b) the information, or other matter, on which that knowledge or suspicion is based came to his attention in the course of his trade, profession, business or employment, and

(c) he does not disclose the information or other matter to a constable as soon as is reasonably practicable

after it comes to his attention.

(2) Subsection (1) does not make it an offence for a professional legal adviser to fail to disclose any information or other matter which has come to him in privileged circumstances.

(3) It is a defence to a charge of committing an offence under this section that the person charged had a reasonable excuse for not disclosing the information or other matter in question.

(4) Where a person discloses to a constable-

(a) his suspicion or belief that another person is engaged in drug money laundering, or

(b) any information or other matter on which that suspicion or belief is based,

the disclosure shall not be treated as a breach of any restriction imposed by statute or otherwise.

(5) Without prejudice to subsection (3) or (4), in the case of a person who was in employment at the time in question, it is a defence to a charge of committing an offence under this section that he disclosed the information or other matter in question to his employer or, where his employer has established a procedure for the making of such disclosures, to the appropriate person in accordance with the procedure.

(6) A disclosure to which subsection (5) applies shall not be treated as a breach of any restriction imposed by statute or otherwise.

(7) In this section 'drug money laundering' means doing any act-

(a) which constitutes an offence under section 45, 46 or 47; or

(b) in the case of an act done otherwise than in the Island, which would constitute such an offence if done in the Island.

(8) For the purposes of subsection (7), having possession of any property shall be taken to be doing an act in relation to it.

(9) For the purposes of this section, any information or other matter comes to a professional legal adviser in privileged circumstances if it is communicated, or given, to him-

(a) by, or by a representative of, a client of his in connection with the giving by the adviser of legal advice to the client;

(b) by, or by a representative of, a person seeking legal advice from the adviser; or

(c) by any person-

(i)in contemplation of, or in connection with, legal proceedings; and

(ii)for the purpose of those proceedings.

(10) No information or other matter shall be treated as coming to a professional legal adviser in privileged circumstances if it is communicated or given with a view to furthering any criminal purpose.

51 Penalties

(1) A person guilty of an offence under section 45, 46 or 47 shall be liable-

(a) on summary conviction, to imprisonment for a term not exceeding 6 months or to a fine not exceeding £5,000 or to both; and

(b) on conviction on information, to imprisonment for a term not exceeding 14 years or to a fine or to both.

(2) A person guilty of an offence under section 48 or 49 shall be liable 10

(a) on summary conviction, to imprisonment for a term not exceeding 6 months or to a fine not exceeding £5,000 or to both; or

(b) on conviction on information, to imprisonment for a term not exceeding 5 years or to a fine or to both.

(3) A person guilty of an offence under section 50 shall be liable on summary conviction to imprisonment for a term not exceeding 6 months or to a fine not exceeding £5,000 or to both.

Anti-Terrorism and Crime Act (ATCA) 2003

4. Support

(1) A person commits an offence if —

(a) he invites support for a proscribed organisation, and

(b) the support is not, or is not restricted to, the provision of money or other property (within the meaning of section 6).

(2) A person commits an offence if he arranges, manages or assists in arranging or managing a meeting which he knows is —

(a) to support a proscribed organisation,

(b) to further the activities of a proscribed organisation, or

(c) to be addressed by a person who belongs or professes to belong to a proscribed organisation.

(3) A person commits an offence if he addresses a meeting and the purpose of his address is to encourage support for a proscribed organisation or to further its activities.

(4) Where a person is charged with an offence under subsection

(2)(c) in respect of a private meeting it is a defence for him to prove that he had no reasonable cause to believe that the address mentioned in subsection

(2)(c) would support a proscribed organisation or further its activities.

(5) In subsections (2) to (4) —

(a) "meeting" means a meeting of 3 or more persons, whether or not the public are admitted, and

(b) a meeting is private if the public are not admitted.

(6) A person guilty of an offence under this section shall be liable

—

(a) on conviction on information, to custody for a term not exceeding 10 years, to a fine or to both, or

(b) on summary conviction, to custody for a term not exceeding 6 months, to a fine not exceeding £5,000 or to both.

6. Terrorist property

(1) In this Act "terrorist property" means —

(a) money or other property which is likely to be used for the purposes of terrorism (including any resources of a proscribed organisation),

(b) proceeds of the commission of acts of terrorism, and

(c) proceeds of acts carried out for the purposes of terrorism.

(2) In subsection (1) —

(a) a reference to proceeds of an act includes a reference to any property which wholly or partly, and directly or indirectly, represents the proceeds of the act (including payments or other rewards in connection with its commission), and

(b) the reference to an organisation's resources includes a reference to any money or other property which is applied or made available, or is to be applied or made available, for use by the organisation.

7. Fund-raising

(1) A person commits an offence if he —

(a) invites another to provide money or other property, and

(b) intends that it should be used, or has reasonable cause to suspect that it may be used, for the purposes of terrorism.

(2) A person commits an offence if he —

(a) receives money or other property, and

(b) intends that it should be used, or has reasonable cause to suspect that it may be used, for the purposes of terrorism.

(3) A person commits an offence if he —(a) provides money or other property, and

(b) knows or has reasonable cause to suspect that it will or may be used for the purposes of terrorism.

(4) In this section a reference to the provision of money or other property is a reference to its being given, lent or otherwise made available, whether or not for consideration.

(5) A person guilty of an offence under this section shall be liable

—

(a) on conviction on information, to custody for a term not exceeding 14 years, to a fine or to both, or

(b) on summary conviction, to custody for a term not exceeding 6 months, to a fine not exceeding £5,000 or to both.

8. Use and possession

(1) A person commits an offence if he uses money or other property for the purposes of terrorism.

(2) A person commits an offence if he —

(a) possesses money or other property, and

(b) intends that it should be used, or has reasonable cause to suspect that it may be used, for the purposes of terrorism.

(3) A person guilty of an offence under this section shall be liable —

(a) on conviction on information, to custody for a term not exceeding 14 years, to a fine or to both, or

(b) on summary conviction, to custody for a term not exceeding 6 months, to a fine not exceeding £5,000 or to both.

9. Funding arrangements

(1) A person commits an offence if —

(a) he enters into or becomes concerned in an arrangement as a result of which money or other property is made available or is to be made available to another, and

(b) he knows or has reasonable cause to suspect that it will or may be used for the purposes of terrorism.

(2) A person guilty of an offence under this section shall be liable

—

(a) on conviction on information, to custody for a term not exceeding 14 years, to a fine or to both, or

(b) on summary conviction, to custody for a term not exceeding 6 months, to a fine not exceeding £5,000 or to both.

10. Money laundering

(1) A person commits an offence if he enters into or becomes concerned in an arrangement which facilitates the retention or control by or on behalf of another person of terrorist property —

(a) by concealment,

(b) by removal from the jurisdiction,

(c) by transfer to nominees, or

(d) in any other way.

(2) It is a defence for a person charged with an offence under subsection (1) to prove that he did not know and had no reasonable cause to suspect that the arrangement related to terrorist property.

(3) A person guilty of an offence under this section shall be liable —

(a) on conviction on information, to custody for a term not exceeding 14 years, to a fine or to both, or

(b) on summary conviction, to custody for a term not exceeding 6 months, to a fine not exceeding £5,000 or to both.

11. Disclosure of information: duty

(1) This section applies where a person —

(a) believes or suspects that another person has committed an offence under any of sections 7 to 10, and

(b) bases his belief or suspicion on information which comes to his attention in the course of a trade, profession, business or employment, but does not apply if the information came to the person in the course of a business in the regulated sector.

(2) The person commits an offence if he does not disclose to a constable as soon as is reasonably practicable —

(a) his belief or suspicion, and

(b) the information on which it is based.

(3) It is a defence for a person charged with an offence under subsection (2) to prove that he had a reasonable excuse for not making the disclosure.

(4) Where —

(a) a person is in employment,

(b) his employer has established a procedure for the making of disclosures of the matters specified in subsection (2), and

(c) he is charged with an offence under that subsection, it is a defence for him to prove that he disclosed the matters specified in that subsection in accordance with the procedure.

(5) Subsection (2) does not require disclosure by a professional legal adviser of —

(a) information which he obtains in privileged circumstances, or

(b) a belief or suspicion based on information which he obtains in privileged circumstances.

(6) For the purpose of subsection (5) information is obtained by an adviser in privileged circumstances if it comes to him, otherwise than with a view to furthering a criminal purpose ,,

(a) from a client or a client's representative, in connection with the provision of legal advice by the adviser to the client,

(b) from a person seeking legal advice from the adviser, or from the person's representative, or

(c) from any person, for the purpose of actual or contemplated legal proceedings.

(7) For the purposes of subsection (1)(a) a person shall be treated as having committed an offence under one of sections 7 to 10 if —

(a) he has taken an action or been in possession of a thing, and

(b) he would have committed an offence under one of those sections if he had been in the Island at the time when he took the action or was in possession of the thing.

(8) In this section —

(a) the reference to a business in the regulated sector must be construed in accordance with Schedule 1,
(b) the reference to a constable includes a reference to a person authorised for the purposes of this section by the Attorney General.

(9) A person guilty of an offence under this section shall be liable

—

(a) on conviction on information, to custody for a term not exceeding 5 years, to a fine or to both, or

(b) on summary conviction, to custody for a term not exceeding 6 months, or to a fine not exceeding £5,000 or to both.

12. Disclosure of information: permission

(1) A person may disclose to a constable —

(a) a suspicion or belief that any money or other property is terrorist property or is derived from terrorist property;

(b) any matter on which the suspicion or belief is based. (2) A person may make a disclosure to a constable in the circumstances mentioned in section 11(1) and (2).

(3) Subsections (1) and (2) shall have effect notwithstanding any restriction on the disclosure of information imposed by statute or otherwise.

(4) Where —

(a) a person is in employment, and

(b) his employer has established a procedure for the making of disclosures of the kinds mentioned in subsection (1) and section 11(2), subsections (1) and (2) shall have effect in relation to that person as if any reference to disclosure to a constable included a reference to disclosure in accordance with the procedure.

(5) In this section, references to a constable include references to a person authorised for the purposes of this section by the Attorney General.

13. Co-operation with police

(1) A person does not commit an offence under any of sections 7 to 10 if he is acting with the express consent of a constable.

(2) Subject to subsections (3) and (4), a person does not commit an offence under any of sections 7 to 10 by involvement in a transaction or arrangement relating to money or other property if he discloses to a constable

—

(a) his suspicion or belief that the money or other property is terrorist property, and

(b) the information on which his suspicion or belief is based. (3) Subsection (2) applies only where a person makes a disclosure

—

(a) after he becomes concerned in the transaction concerned,

(b) on his own initiative, and

(c) as soon as is reasonably practicable.

(4) Subsection (2) does not apply to a person if —

(a) a constable forbids him to continue his involvement in the transaction or arrangement to which the disclosure relates, and

(b) he continues his involvement.

(5) It is a defence for a person charged with an offence under any of sections 7(2) and (3) and 8 to 10 to prove that —

(a) he intended to make a disclosure of the kind mentioned in subsections (2) and (3), and

(b) there is reasonable excuse for his failure to do so.

(6) Where —

(a) a person is in employment, and

(b) his employer has established a procedure for the making ofdisclosures of the same kind as may be made to a constable under subsection (2), this section shall have effect in relation to that person as if any reference to disclosure to a constable included a reference to disclosure in accordance with the procedure.

(7) A reference in this section to a transaction or arrangement relating to money or other property includes a reference to use or possession.

14. Failure to disclose: regulated sector

(1) A person commits an offence if each of the following three conditions is satisfied.

(2) The first condition is that he —

(a) knows or suspects, or

(b) has reasonable grounds for knowing or suspecting, that another person has committed an offence under any of sections 7 to 10.

(3) The second condition is that the information or other matter —

(a) on which his knowledge or suspicion is based, or

(b) which gives reasonable grounds for such knowledge or suspicion, came to him in the course of a business in the regulated sector.

(4) The third condition is that he does not disclose the information or other matter to a constable or a nominated officer as soon as is practicable after it comes to him.

(5) But a person does not commit an offence under this section if

—

(a) he has a reasonable excuse for not disclosing the information or other matter;

(b) he is a professional legal adviser and the information or other matter came to him in privileged circumstances.

(6) In deciding whether a person committed an offence under this section the court must consider whether he followed any relevant guidance which was at the time concerned —

(a) issued by a supervisory authority or any other appropriate body, and

(b) approved by the Treasury, and

(c) published in a manner it approved as appropriate in its opinion to bring the guidance to the attention of persons likely to be affected by it.

(7) A disclosure to a nominated officer is a disclosure which —

(a) is made to a person nominated by the alleged offender's employer to receive disclosures under this section, and

(b) is made in the course of the alleged offender's employment and in accordance with the procedure established by the employer for the purpose.

(8) Information or other matter comes to a professional legal adviser in privileged circumstances if it is communicated or given to him —

(a) by (or by a representative of) a client of his in connection with the giving by the adviser of legal advice to the client,

(b) by (or by a representative of) a person seeking legal advice from the adviser, orby a person in connection with legal proceedings or contemplated legal proceedings.

(9) But subsection (8) does not apply to information or other matter which is communicated or given with a view to furthering a criminal purpose.

(10) Schedule 1 has effect for the purpose of determining what is — (a) a business in the regulated sector;

(b) a supervisory authority.

(11) For the purposes of subsection (2) a person is to be taken to have committed an offence under one of sections 7 to 10 if —

(a) he has taken an action or been in possession of a thing, and

(b) he would have committed the offence if he had been in the Island at the time when he took the action or was in possession of the thing.

(12) A person guilty of an offence under this section is liable —

(a) on conviction on information, to custody for a term not exceeding 5 years or to a fine or to both;

(b) on summary conviction, to custody for a term not exceeding 6 months or to a fine not exceeding £5,000 or to both.

(13) An appropriate body is any body which regulates or is representative of any trade, profession, business or employment carried on by the alleged offender.

(14) The reference to a constable includes a reference to a person authorised for the purposes of this section by the Attorney General.

16. Forfeiture

(1) The court by or before which a person is convicted of an offence under any of sections 7 to 10 may make a forfeiture order in accordance with the provisions of this section.

(2) Where a person is convicted of an offence under section 7(1) or

(2) or 8 the court may order the forfeiture of any money or other property —

(a) which, at the time of the offence, he had in his possession or under his control, and

(b) which, at that time, he intended should be used, or had reasonable cause to suspect might be used, for the purposes of terrorism.

(3) Where a person is convicted of an offence under section 7(3) the court may order the forfeiture of any money or other property —

(a) which, at the time of the offence, he had in his possession or under his control, and(b) which, at that time, he knew or had reasonable cause to suspect would or might be used for the purposes of terrorism.

(4) Where a person is convicted of an offence under section 9 the court may order the forfeiture of the money or other property —

(a) to which the arrangement in question related, and

(b) which, at the time of the offence, he knew or had reasonable cause to suspect would or might be used for the purposes of terrorism.

(5) Where a person is convited of an offence under section 10 the court may order the forfeiture of the money or other property to which the arrangement in question related.

(6) Where a person is convicted of an offence under any of sections 7 to 10, the court may order the forfeiture of any money or other property which wholly or partly, and directly or indirectly, is received by any person as a payment or other reward in connection with the commission of the

offence.

(7) Where a person other than the convicted person claims to be the owner of or otherwise interested in anything which can be forfeited by an order under this section, the court shall give him an opportunity to be heard before making an order.

(8) Schedule 2 (which makes further provision in relation to forfeiture orders under this section) shall have effect.

26. Information about acts of terrorism

(1) This section applies where a person has information which he knows or believes might be of material assistance —

(a) in preventing the commission by another person of an act of terrorism, or

(b) in securing the apprehension, prosecution or conviction of another person, in the Island, for an offence involving the commission, preparation or instigation of an act of terrorism.

(2) The person commits an offence if he does not disclose the information as soon as reasonably practicable in accordance with subsection (3).

(3) Disclosure is in accordance with this subsection if it is made to a constable.

(4) It is a defence for a person charged with an offence under subsection (2) to prove that he had a reasonable excuse for not making the disclosure.

(5) A person guilty of an offence under this section shall be liable

(a) on conviction on information, to custody for a term not exceeding 5 years, or to a fine or to both, or

(b) on summary conviction, to custody for a term not exceeding 6 months, or to a fine not exceeding £5,000 or to both.

(6) Proceedings for an offence under this section may be taken, and the offence may for the purposes of those proceedings be treated as having been committed, in any place where the person to be charged is or has at any time been since he first knew or believed that the information might be of material assistance as mentioned in subsection (1).

Schedule 3 Part 2

SEIZURE AND DETENTION

Seizure of cash

2. (1) An authorised officer may seize any cash if he has reasonable grounds for suspecting that it is terrorist cash.

(2) An authorised officer may also seize cash part of which he has reasonable grounds for suspecting to be terrorist cash if it is not reasonably practicable to seize only that part.

Detention of seized cash

3. (1) While the authorised officer continues to have reasonable grounds for his suspicion, cash seized under this Schedule may be detained initially for a period of 48 hours.

(2) The period for which the cash or any part of it may be detained may be extended by an order made by the High Bailiff; but the order may not authorise the detention

(a) beyond the end of the period of 3 months beginning with the date of the order,

(b) in the case of any further order under this paragraph, beyond the end of the period of 2 years beginning with the date of the first order.

(3) An order under sub-paragraph (2) must provide for notice to be given to persons affected by it.

(4) An application for an order under sub-paragraph (2) may be made by the Treasury or an authorised officer, and the High Bailiff may make the order if satisfied, in relation to any cash to be further detained, that one of the following conditions is met.

5) The first condition is that there are reasonable grounds for suspecting that

(a) its continued detention is justified while its intended use is further investigated or consideration is given to bringing (in the Island or elsewhere) proceedings against any person for an offence with which the cash is connected, or

(b) proceedings against any person for an offence with which the cash is connected have been started and have not been concluded.

(6) The second condition is that there are reasonable grounds for suspecting that the cash consists of resources of a proscribed organisation and that either

(a) its continued detention is justified while investigation is made into whether or not it consists of such resources or consideration is given to bringing (in the Island or elsewhere) proceedings against any person for an offence with which the cash is connected, or

(b) proceedings against any person for an offence with which the cash is connected have been started and have not been concluded.

(7) The third condition is that there are reasonable grounds for suspecting that the cash is property earmarked as terrorist property and that either û

(a) its continued detention is justified while its derivation is further investigated or consideration is given to bringing (in the Island or elsewhere) proceedings against any person for an offence with which the cash is connected, or

(b) proceedings against any person for an offence with which the cash is connected have been started and have not been concluded.

7. (1) A constable may seize any property subject to a restraint order for the purpose of preventing it from being removed from the Island.

(2) Property seized under this paragraph shall be dealt with in accordance with the High Court's directions.

8. (1) The Land Registration Act 1982

(a) shall apply in relation to restraint orders as it applies in relation to orders affecting land made by the court for the purpose of enforcing judgments or recognizances, and

(b) shall apply in relation to applications for restraint orders as it applies in relation to other pending land actions.

(2) Where a restraint order is made under paragraph 5(1) or an application for such an order is made, the prosecutor in the proceedings for the offence shall be treated for the purposes of section 62 of the Land Registration Act 1982 (inhibitions) as a person interested in respect of any registered land to which the restraint order or the application for the restraint order relates.

(3) Where a restraint order is made under paragraph 5(2) or an application for such an order is made, the person who the High Court is satisfied will have the conduct of any proceedings for an offence under any of sections 7 to 10 shall be treated for the purposes of section 62 of that Act as a person interested in respect of any registered land to which the restraint order or the application for the restraint order relates.

Anti-Terrorism (Enforcement of External Orders) Order 2004

Registration of external forfeiture orders

9. (1) On an application made by or on behalf of the government of a designated country, the High Court may register an external forfeiture order made there if -

(a) it is satisfied that at the time of registration the order is in force and not subject to appeal,

(b) it is satisfied, where the person against whom the order is made did not appear in the proceedings in which the relevant order was made, that he received notice of the proceedings in sufficient time to enable him to defend them, and

(c) it is of the opinion that enforcing the order in the Island would not be contrary to the interests of justice.

(2) In paragraph (1) above, "appeal" includes -

(a) any proceedings by way of discharging or setting aside a judgement, and

(b) an application for a new trial or a stay of execution.

Registration of external restraint orders10. (1) On an application made by or on behalf of the Government of a designated country, the High Court may, subject to paragraph (2) below, register an external restraint order made there if -

(a) it is satisfied that at the time of registration the order is in force, and

(b) it is of the opinion that enforcing the order in the Island would not be contrary to the interests of justice.

(2) An external restraint order may only be registered where -

(a) proceedings have been instituted against a person in a designated country, the proceedings have not been concluded, and either an external forfeiture order has been made in the proceedings or it appears to the High Court that there are reasonable grounds for thinking that such an order may be made in those proceedings, or

(b) proceedings are to be instituted against a person in a designated country and there are reasonable grounds for thinking that an external forfeiture order may be made in those proceedings.

Criminal Law Act 1981

16 Power to deprive offender of property used, or intended for use, for purposes of crime

(1) Where a person is convicted of an offence and-

(a) the court by or before which he is convicted is satisfied that any property which has been lawfully seized from him or which was in his possession or under his control at the time when he was apprehended for the offence or when a summons in respect of it was issued-

(i)has been used for the purpose of committing, or facilitating the commission of, any offence; or

(ii)was intended by him to be used for that purpose; or

(b) the offence, or an offence which the court has taken into account in determining his sentence, consists of unlawful possession of property which has been lawfully seized from him or which was in his possession or under his control at the time when he was apprehended for the offence or when a summons in respect of it was issued,

the court may make an order under this section in respect of that property and may do so whether or not it also deals with the offender in respect of the offence in any other way and without regard to any restrictions on forfeiture in any Act passed before the Criminal Justice Act 1990.

(1A) In considering whether to make an order under subsection (1) in respect of any property a court shall have regard-

(a) to the value of the property; and

(b) to the likely effects on the offender of the making of the order (taken together with any other order that the court contemplates making).

(2) Facilitating the commission of an offence shall be taken for the purposes of this section and section 17 to include the taking of any steps after it has been committed for the purpose of disposing of any property to which it relates or of avoiding apprehension or detection, and references in this or that section to an offence punishable with imprisonment shall be construed without regard to any prohibition or restriction imposed by or under any enactment on the imprisonment of young offenders.

(3) An order under this section shall operate to deprive the offender of his rights (if any) in the property to which it relates, and the property shall (if not already in their possession) be taken into the possession of the police.

(4) Section 34 of the Summary Jurisdiction Act 1989 shall apply, with the following modifications, to property which is in the possession of the police by virtue of this section-

(a) no application shall be made under subsection (1) of that section by any claimant of the property after the expiration of six months from the date on which the order in respect of the property was made under this section; and

(b) no such application shall succeed unless the claimant satisfies the court either that he had not consented to the offender having possession of the property or, where an order is made under subsection (1)*(a)*, that he did not know, and had no reason to suspect, that the property was likely to be used for the purpose mentioned in that paragraph.

(5) In relation to property which is in the possession of the police by virtue of this section and in respect of which no application has been made within the period specified in subsection (4)*(a)* or no such application has succeeded, section 34(1) of the said Act of 1989 shall apply as if the owner of the property cannot be ascertained.

Misuse of Drugs Act 1976

27 Forfeiture

(1) Subject to subsection (2) below, the court by or before which a person is convicted of an offence to which this section applies may order anything shown to the satisfaction of the court to relate to the offence, to be forfeited and either destroyed or dealt with in such other manner as the court may order.

(1A) This section applies to any offence which is either (or both) of the following-

(a) an offence under this Act;

(b) a drug trafficking offence, as defined in section 1(3) of the Drug Trafficking Act 1996.

(2) The court shall not order anything to be forfeited under this section, where a person claiming to be the owner of or otherwise interested in it applies to be heard by the court, unless an opportunity has been given to him to show cause why the order should not be made.

Al-Qa'ida and Taliban (United Nations Measures)(Isle of Man) Order 2002

Freezing of funds

8.—(1) Where the Treasury has reasonable grounds for suspecting that the person by, for or on behalf of whom any funds are held is or may be a listed person or a person acting on behalf of a listed person, the Treasury may by notice direct that those funds are not to be made available to any person, except under the authority of a licence granted by the Treasury under article 7.

(2) A direction given under paragraph (1) shall specify either—

(a) the period for which it is to have effect, or

(b) that the direction is to have effect until it is revoked by notice under paragraph (3).

(3) The Treasury may by notice revoke a direction given under paragraph (1) at any time.

(4) The expiry or revocation of a direction shall not affect the application of article 7 in respect of the funds in question.

(5) A notice under paragraph (1) or (3) shall be given in writing to the person holding the funds in question ("the recipient"), and shall require the recipient to send a copy of the notice without delay to the person whose funds they are, or on whose behalf they are held ("the owner").

(6) A recipient shall be treated as complying with that requirement if, without delay, he sends

a copy of the notice to the owner at his last-known address or, if he does not have an address for the owner, he makes arrangements for a copy of the notice to be supplied to the owner at the first available opportunity.

(7) Any person whose funds are the subject of a direction made under paragraph (1) above, may apply for the direction to be reviewed in the same manner as the review of a direction under the Banking Act 1998 (an Act of Tynwald), and section 24 of that Act and any regulations under that section shall apply to a review under this Order as they apply in respect of a review under that section.

(8) Any person who contravenes a direction under paragraph (1) is guilty of an offence.

(9) A recipient who fails to comply with such a requirement as is mentioned in paragraph (5) is guilty of an offence.

Terrorism (United Nations Measures)(Isle of Man) Order 2001

Freezing of funds on suspicion

6.—(1) Where the Treasury have reasonable grounds for suspecting that the person by, for, or on behalf of whom any funds are held is or may be—

(a) a person who commits, attempts to commit, participates in, or facilitates the commission of terrorism,

(b) a person controlled or owned directly or indirectly by a person referred to in subparagraph (a) above,

(c) a person acting on behalf of, or at the direction of a person referred to in subparagraph (a) above,

the Treasury may by notice direct that those funds are not to be made available to any person, except under the authority of a licence granted by the Treasury under this article.

(2) A notice given under paragraph (1) shall specify either—

(a) the period for which it is to have effect, or

(b) that the direction is to have effect until it is revoked by notice under paragraph (3) below.

(3) The Treasury may by notice revoke a direction under paragraph (1) at any time.

(4) The expiry or revocation of a direction shall not affect the application of article 5 in respect of the funds in question.

(5) A notice under paragraph (1) or (3) shall be given in writing to the person holding the funds in question ("the recipient"), and shall require the recipient to send a copy of the notice without delay to the person whose funds they are, or on whose behalf they are held ("the owner").

(6) A recipient shall be treated as complying with that requirement if, without delay, he sends a copy of the notice to the owner at his last-known address or, if he does not have an address for the owner, he makes arrangements for a copy of the notice to be supplied to the owner at the first available opportunity.

3(7) Any person whose funds are the subject of a direction made under paragraph (1) above, may apply for the direction to be reviewed in the same manner as the review of a direction under the Banking Act 1989 (an Act of Tynwald), and section 24 of that Act and any regulations under that section shall apply to a review under this Order as they apply in respect of a review under that section.

(8) Any person who contravenes a direction under paragraph (1) above shall be guilty of an offence.

(9) A recipient who fails to comply with such a requirement as is mentioned in paragraph

(6) shall be guilty of an offence.

Customs and Excise Management Act 1986

76C. (1) A person entering or leaving the Island and carrying, or otherwise having in their possession or control, cash with a value in excess of the prescribed amount must declare that value to an officer.

(2) The Treasury must by order prescribe the form and manner in which declarations under

subsection (1) are to be made.

(3) An officer may require a person entering or leaving the Island –

(a) to disclose the value of any cash –

(i) contained in his or her baggage;

(ii) carried with the person; or

(iii) contained in any vehicle in which the person is travelling;

(b) to answer questions in respect of any such cash; and

(c) to produce his or her baggage for inspection by the officer.

(4) The Treasury may by order prescribe the form and manner in which disclosures under subsection (3)(a) are to be made.

(5) A person who, when required to produce his or her baggage, refuses or fails to do so, commits an offence and is liable –(a) on summary conviction, to custody for a term not exceeding 6 months, or to a fine not exceeding £5,000, or to both; or

(b) on conviction on information, to custody for a term not exceeding 2 years, or to a fine, or to both.

(6) Where an officer reasonably suspects that a person entering or leaving the Island is carrying cash with a value in excess of the prescribed amount, the officer may –

(a) where the officer is of the same sex as the person, search the person; or

(b) request an officer of the same sex as the person to do so.

(7) A person who is searched may require to be taken before a justice of the peace or a superior officer who must –

(a) consider the grounds for the officer's suspicion; and

(b) direct whether the search is to take place.

(8) This section does not require a person to submit to an intimate search or strip search (within the meaning of section 171).

Companies Act 2006

30. (1) A company has no power to, and shall not —

(a) issue a bearer share;

(b) convert a share to a bearer share; or

(c) exchange a share for a bearer share, and, accordingly, any such purported issue, conversion or exchange shall be void and of no effect.

(2) A company that attempts or purports to contravene subsection (1) commits an offence.

74. (1) A company shall at all times have a registered agent in the Isle of Man.

(2) Unless the last registered agent of the company has resigned in accordance with section 76 or ceased to be the company's registered agent in accordance with section 77, the registered agent of a company is —

(a) the person specified as the company's first registered agent in the memorandum filed under section 5(1), section 144(1) section 149(1), section 154(2), section 157(3) or section 162(3), as the case may be; or (b) if one or more notices of change of registered agent have been filed under section 75, the person specified as the company's registered agent in the last such notice to be registered by the Registrar.

(3) No person shall be, or agree to be, the registered agent of a company unless that person holds a licence granted under the Fiduciary Services Acts 2000 and 2005 which does not exclude acting as registered agent.

(4) Subject to section 77(6), a person who contravenes subsection (3) commits an offence.

(5) A company that does not have a registered agent commits an offence.

Companies Act 1931-2004

71 Prohibition of share warrants to bearer

(1) Any provision in the memorandum or articles of a company registered on or after 1st April 2004 which purports to authorise the issue of a warrant stating that the bearer is entitled to the shares therein specified, shall be void.

(2) A warrant as described in subsection (1) shall be termed a 'share warrant'.

(3) Subject to subsection (4), in the case of any company registered before 1st April 2004 any provision in its memorandum or articles which authorises, or is capable of authorising, the issue of share warrants on or after 1st April 2004 shall be void.

(4) Any share warrant lawfully issued on or before 1st April 2004 shall remain valid in respect of the rights and obligations attached to it and which may accrue thereafter save that no rights attached to a

share warrant may be exercised by the holder of a share warrant after that date without the conversion of the share warrant into a registered share.

Extradition Act 1989

2. (l) In this Act, except in Schedule 1, "extradition crime" means—

(a) conduct in the terntory of a foreign state, a designated Commonwealth country or a colony which, if it occurred in the United Kingdom, would constitute an offence punishable with

imprisonment for a term of 12 months, or any greater punishment, and which, however described in the law of the foreign state, Commonwealth country or colony, punishable under that law;

(b) an extra-territorial offence against the law of a foreign state, designated Commonwealth country or colony which is punishable under that law with imprisonment for a term of 12 months, or any greater punishment, and which satisfies—

(i) the condition specified in subsection (2) below; or

(ii) all the conditions specified in subsection (3) below.

(2) The condition mentioned in subsection (1)(b)(i) above is that in corresponding circumstances equivalent conduct would constitute an extra-territorial offence against the law of the United Kingdom

punishable with imprisonment for a term of 12 months, or any greater punishment.

(3) The conditions mentioned in subsection (1)(b)(ii) above are—

(a) that the foreign state, Commonwealth country or colony bases its jurisdiction on the nationality of the offender;

(b) that the conduct constituting the offence occurred outside the United Kingdom; and

(c) that, if it occurred in the United Kingdom, it would constitute an offence under the law of the United Kingdom punishable with imprisonment for a term of 12 months, or any greater punishment. (4) For the purposes of subsections (1) to (3) above—

(a) the law of a foreign state, designated Commonwealth country or colony includes the law of any part of it and the law of the United Kingdom includes the law of any part of the United

Kingdom;

(b) conduct in a colony or dependency of a foreign state or of a PART I designated Commonwealth country, or a vessel, aircraft or hovercraft of a foreign state or of such a country, shall be

treated as if it were conduct in the territory of that state or country; and

(c) conduct in a vessel, aircraft or hovercraft of a colony of the United Kingdom shall be treated as if it were conduct in that colony.

PROCEEDS OF CRIME ACT 2008

Arrangement of Sections

PART 1

CIVIL RECOVERY OF THE PROCEEDS ETC. OF UNLAWFUL CONDUCT

Chapter 1

Introductory

Chapter 2

Civil recovery in the High Court

Proceedings for recovery orders

Property freezing orders

Interim receiving orders

PART 4

INVESTIGATIONS

Chapter 1

Introduction

Chapter 2

Investigation provisions

Courts

Production orders

Search and seizure warrants

Disclosure orders

Customer information orders

Account monitoring orders

Evidence overseas

PART 10

MISCELLANEOUS AND GENERAL

Miscellaneous

General

Statutory Document No. 935/08

CRIMINAL JUSTICE ACT 1990

CRIMINAL JUSTICE (MONEY LAUNDERING) CODE 2008

INDEX

Record Keeping

Staff, Training and Technological Developments

Statutory Document No. 935/08

CRIMINAL JUSTICE ACT 1990

CRIMINAL JUSTICE (MONEY LAUNDERING) CODE 2008

Laid before Tynwald: 16th December 2008

Coming into operation: 18th December 2008

The Department of Home Affairs makes this Code under section 17F of the Criminal Justice Act 1990[1] and after consulting such persons and bodies as it considered appropriate.

1 Title and commencement

The title of this Code is the Criminal Justice (Money Laundering) Code 2008 and it shall come into operation on 18th December 2008.

2 Interpretation and revocation

(1) In this Code —

"applicant for business" means a person seeking to form a business relationship or carry out a one-off transaction with a relevant person who is carrying on relevant business in or from the Island;

"beneficial owner" means the natural person who ultimately owns or controls the applicant for business or on whose behalf a transaction or activity is being conducted; and in relation to a legal person or legal arrangement, 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 (whether through direct or indirect ownership or control, including through bearer share

[1] 1990 c.1

Price £3.40

holdings) more than 25% of the shares or voting rights in the legal person; or

(b) in the case of any legal person, a natural person who otherwise exercises control over the management of the legal person;

(c) in the case of a legal arrangement the trustees or other persons controlling the applicant;

"business relationship" means an arrangement between two or more persons where —

(a) at least one of those persons is acting in the course of a business;

(b) the purpose of the arrangement is to facilitate the carrying out of transactions between the persons concerned on a frequent, habitual or regular basis; and

(c) the total amount of any payment or payments to be made by any person to any other in the course of that arrangement is not known or capable of being ascertained at the time the arrangement is made;

"competent authority" means all Isle of Man administrative and law enforcement authorities concerned with combating money laundering and terrorist financing, including; the Financial Supervision Commission, the Insurance and Pensions Authority, the Isle of Man Gambling Supervision Commission, the Department of Home Affairs, the Financial Crime Unit of the Isle of Man Constabulary, the Office of Fair Trading, Customs and Excise;

"constable" includes an officer under the Customs and Excise Management Act 1986[2];

"correspondent banking services" means banking services provided by a financial institution in one country ("the correspondent bank") to a financial institution in another country ("the respondent bank");

"country" includes territory;

"customer due diligence" (except in the expression "enhanced customer due diligence") means the measures specified in paragraphs 5 to 7 and 9 to 15 of the Code;

"deposit taking" has the meaning given in section 3 of the Financial Services Act 2008[3] and Class 1 of Schedule 1 to the Regulated Activities Order 2008[4], ignoring any exclusions from that class contained within the Order or any exemptions contained with the Financial Services

[2] 1986 c.34
[3] 2008 c.8
[4] SD 367/08

(Exemption) Regulations 2008[5];

"director" and "officer" of a body corporate include, in the case of a limited liability company constituted under the Limited Liability Companies Act 1996[6], a member, manager or registered agent of such a company;

"exempted one-off transaction" means a one-off transaction (whether a single transaction or a series of linked transactions) where the amount of the transaction or, as the case may be, the aggregate in the case of a series of linked transactions, is less in value than —

(a) euro 3,000 in the case of a transaction or series of linked transactions entered into in the course of business of a class specified in entries 9 and 11 in Schedule 1; or

(b) euro 15,000 in any other case;

"external regulated business" means business outside the Island that corresponds to business carried out by a regulated person and which is regulated or supervised by an authority (whether a governmental or private body and whether in the Island or in a country outside the Island) which is empowered (whether by law or by the rules of the body) to regulate or supervise such business;

"FATF Recommendations" means the 40 Recommendations of the Financial Action Task Force on Money Laundering and the Task Force's 9 Special Recommendations on Terrorist Financing;

"insurer" means an insurer who is authorised under section 8 of the Insurance Act 2008[7] or which holds a permit under section 22 of the Insurance Act 2008;

"insurance business" has the same meaning as in the Insurance Act 2008;

"investment business" has the meaning given in section 3 of the Financial Services Act 2008 and Class 2 of Schedule 1 to the Regulated Activities Order 2008 ignoring any exclusions for that class contained within the Order or exemptions contained with the Financial Services (Exemptions) Regulations 2008;

"legal arrangement" means —

(a) an express trust, or

[5] SD 368/08
[6] 1996 c.19
[7] 2008 c.16

(b) any other arrangement which has a similar legal effect (such as a *fiducie, Treuhand* or *fideicomiso*);

"legal person" includes any body corporate or unincorporate which is capable of establishing a permanent customer relationship with a financial institution or of owning property;

"money laundering reporting officer" ("MLRO") means an individual appointed under paragraph 20 of this Code;

"money laundering" includes any act in contravention of the money laundering requirements;

"the Money Laundering Directive" means Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing;

"the money laundering requirements" means the requirements of the following enactments —

(a) sections 45 to 49 of the Drug Trafficking Act 1996[8];

(b) sections 17A to 17D and 17K of the Criminal Justice Act 1990;

(c) section 9 of the Prevention of Terrorism Act 1990[9]; and

(d) sections 7 to 11 and section 14 of the Anti-Terrorism and Crime Act 2003[10],

and includes, in the case of anything done otherwise than in the Island, anything which would constitute an offence under the provisions specified in paragraphs (a) to (d) if done in the Island and references to "anti-money laundering requirements" shall be construed accordingly;

"one-off transaction" means any transaction other than a transaction carried out in the course of an established business relationship formed by a relevant person and, for the purposes of this definition, a business relationship is an established business relationship if it is formed by a relevant person where that person has obtained under procedures established, maintained and operated in accordance with this Code, satisfactory evidence of the identity of the person who, in relation to the formation of that business relationship, was the applicant for business;

"payable-through account" means an account maintained by a correspondent bank which may be operated directly by a customer of the respondent bank;

[8] 1996 c.3
[9] 1990 c.19 (Although the Act is repealed, it is possible for proceedings to be taken in respect of acts undertaken when it was in force)
[10] 2003 c.6

"politically exposed person" means any of the following resident in a country or territory outside the Island —

(a) a natural person who is or has been entrusted with prominent public functions, including —

(i) a head of state, head of government, minister or deputy or assistant minister;

(ii) a senior government official;

(iii) a member of parliament;

(iv) a senior politician;

(v) an important political party official;

(vi) a senior judicial official;

(vii) a member of a court of auditors or the board of a central bank;

(viii) an ambassador, chargé d'affaires or other high-ranking officer in a diplomatic service;

(ix) a high-ranking officer in an armed force;

(x) a senior member of an administrative, management or supervisory body of a State-owned enterprise; and

(xi) a senior official of an international entity or organisation;

(b) any of the following family members of a person mentioned in sub-paragraph (a) —

(i) a spouse;

(ii) a partner considered by national law as equivalent to a spouse;

(iii) a child or the spouse or partner of a child;

(iv) a brother or sister (including a half-brother or half-sister);

(v) a parent;

(vi) a parent-in-law;

(vii) a grandparent; and

(viii) a grandchild;

(c) any close associate of a person mentioned in sub-paragraph (a), including —

(i) any natural person who is known to have joint beneficial ownership of a legal entity or legal arrangement, or any other close business relations, with such a person;

(ii) any natural person who has sole beneficial ownership of a legal entity or legal arrangement which is known to have been set up for the benefit of such a person;

(iii) any natural person who is known to be beneficiary of a legal arrangement of which such a person is a beneficial owner or beneficiary;

(iv) any natural person who is known to be in a position to conduct substantial financial transactions on behalf of such a person;

"regulated person" means —

(a) any person holding a financial services licence issued under section 7 of the Financial Services Act 2008;

(b) any person carrying on insurance business or acting as an insurance manager within the meaning of the Insurance Act 2008;

(c) the trustee of a retirement benefits scheme that is authorised under section 3 of the Retirement Benefits Schemes Act 2000[11]; or

(d) a retirement benefits schemes administrator who is registered under section 36 of the Retirement Benefits Schemes Act 2000;

"relevant business" means engaging by way of business in one or more of the businesses, transactions or activities specified in Schedule 1;

"relevant person" means a person carrying on relevant business.

"risk" means a risk of money laundering or the financing of terrorism, or both;

(2) In this Code, "shell bank" means a bank which is —

(a) incorporated in a country or territory in which it has no physical presence; and

(b) not affiliated with a financial services group which is subject to effective consolidated supervision;

and for this purpose —

[11] 2000 c.14

"consolidated supervision", in relation to a financial services group, means supervision of the group by a regulatory body on the basis of the totality of its business, wherever conducted;

"financial services group" means a group of companies whose activities include to a significant extent activities which are, or if carried on in the Island would be, regulated activities.

(3) The Criminal Justice (Money Laundering) Code 2007[12], the Criminal Justice (Money Laundering) (Amendment) Code 2007[13] and the Criminal Justice (Money Laundering) (Amendment) Code 2008[14] are revoked.

3 Risk assessment

(1) For the purpose of determining the measures to be taken when carrying out customer due diligence, a relevant person must carry out a risk assessment in accordance with this paragraph.

(2) The assessment must estimate the risk of money laundering and terrorist financing on the part of the relevant person's customers, having regard to —

(a) the nature, scale and complexity of its activities;

(b) the products and services provided;

(c) the persons to whom, and the manner in which they are provided; and

(d) reliance on third parties for elements of the customer due diligence process.

(3) The assessment must be —

(a) undertaken as soon as reasonably practicable —

(i) after this Code comes into force, in the case of an existing business; or

(ii) after the relevant person commences business, in any other case; and

(b) regularly reviewed and, where appropriate, amended so as to keep it up to date.

[12] SD 712/07
[13] SD 903/07
[14] SD 296/08

(4) When carrying out customer due diligence, whether in relation to an applicant for business, an existing business relationship or a one-off transaction, a relevant person must do so —

(a) on the basis of materiality and risk;

(b) in accordance with its current risk assessment under this paragraph; and

(c) having regard to whether the applicant for business, an existing business relationship or a one-off transaction poses a higher risk.

4 General requirements

(1) In conducting relevant business a relevant person shall not form a business relationship or carry out a one-off transaction with or for another person nor continue a business relationship unless the relevant person —

(a) establishes, maintains and operates —

(i) identification procedures in accordance with paragraphs 5 to 15;

(ii) record keeping procedures in accordance with paragraphs 16 to 19;

(iii) internal reporting procedures in accordance with paragraph 20;

(iv) internal staff screening procedures in accordance with paragraph 21;

(v) internal controls and communication procedures which are appropriate for the purposes of forestalling and preventing money laundering; and

(vi) procedures and controls in accordance with paragraph 23;

(b) takes appropriate measures from time to time for the purpose of making employees aware of —

(i) the procedures established, maintained and operated under head (a); and

(ii) the provisions of the money laundering requirements; and

(c) provides education and training in accordance with paragraph 22.

(2) Any person who contravenes sub-paragraph (1) shall be guilty of an

offence and liable —

(a) on summary conviction to custody for a term not exceeding 6 months or to a fine not exceeding £5,000, or to both; and

(b) on conviction on information to custody not exceeding 2 years or to a fine, or to both.

(3) In determining whether a person has complied with any of the requirements of sub-paragraph (1), a court may take account of —

(a) any relevant supervisory or regulatory guidance which applies to that person and which is given by a competent authority; or

(b) in a case where no guidance falling within head (a) applies, any other relevant guidance issued by a body that regulates, or is representative of, any trade, business, profession or employment carried on by that person.

(4) In proceedings against a person for an offence under this paragraph, it shall be a defence for that person to show that he took all reasonable steps and exercised all due diligence to avoid committing the offence.

(5) Sub-paragraph (6) applies where an offence under this paragraph is committed by a body corporate and it is proved that the offence —

(a) was committed with the consent or connivance of, or

(b) was attributable to neglect on the part of, an officer of the body.

(6) The officer, as well as the body, shall be guilty of the offence.

(7) Sub-paragraph (8) applies where an offence under this paragraph is committed by a partnership, or by an association other than a partnership or body corporate, and it is proved that the offence —

(a) was committed with the consent or connivance of; or

(b) was attributable to neglect on the part of;

a partner in the partnership or (as the case may be) a person concerned in the management or control of the association.

(8) The partner or (as the case may be) the person concerned, as well as the

partnership or association, shall be guilty of the offence.

(9) Where a person is convicted of an offence under this paragraph by virtue of sub-paragraph (6) or (8), that person shall be liable —

(a) on summary conviction to custody for a term not exceeding 6 months or to a fine not exceeding £5,000, or to both; and

(b) on conviction on information to custody not exceeding 2 years or to a fine, or to both.

(10) In this paragraph "officer" includes —

(a) a director, manager or secretary;

(b) a person purporting to act as a director, manager or secretary;

(c) a member, if the affairs of the body are managed by its members.

IDENTIFICATION PROCEDURES

5 Beneficial ownership and control

(1) This paragraph applies where a relevant person is operating the procedures required by paragraphs 6 to 11 and 15 of the Code.

(2) The relevant person must, in the case of any applicant for business —

(a) identify who is the beneficial owner of the applicant;

(b) take reasonable steps to verify the identity of those persons, using relevant information or data obtained from a reliable source; and

(c) determine whether the applicant is acting on behalf of another person and, if so, identify that other person, and take reasonable steps to verify his identity using relevant information or data obtained from a reliable source.

(3) Without prejudice to sub-paragraph (2), the relevant person must, in the case of an applicant for business which is a legal person or legal arrangement —

(a) verify that any person purporting to act on behalf of the applicant is authorised to do so;

(b) identify that person and take reasonable steps to verify the identity of that person using reliable and independent source documents, data or information;

(c) in the case of a legal arrangement, identify any known beneficiaries;

(d) in the case of a legal arrangement, identify the settlor or other person by whom the legal arrangement is made;

(e) verify the legal status of the applicant using relevant information or data obtained from a reliable source;

(f) obtain information concerning the names and addresses of the applicant and any natural persons having power to direct its activities;

(g) obtain information concerning the person by whom, and the method by which, binding obligations may be imposed on the applicant;

(h) obtain information to understand the ownership and control structure of the applicant.

(4) Without prejudice to sub-paragraphs (2) and (3), the relevant person must not, in the case of an applicant for business which is a legal person or legal arrangement, make any payment to a beneficiary of the arrangement unless it has —

(a) identified the beneficiary; and

(b) verified his identity using relevant information and data obtained from a reliable source.

(5) Where the relevant person deals with an applicant for business otherwise than face-to-face, it must, in taking any steps under this paragraph, take adequate measures to compensate for any risk arising as a result.

(6) In this paragraph "applicant for business", in relation to a continuing business relationship, means the person who, in relation to the formation of the business relationship, was the applicant for business.

6 New business relationships

(1) A relevant person shall establish, maintain and operate the procedures specified in sub-paragraph (3).

(2) Those procedures shall be undertaken —

(a) before a business relationship is entered into; or

(b) during the formation of that relationship,

but in any event as soon as reasonably practicable (taking into account the need not to interrupt the normal conduct of business where there is little risk of money laundering or terrorist financing occurring) after contact is first made between the relevant person and the applicant for business concerning any particular business relationship.

(3) The procedures referred to in sub-paragraph (1) are —

(a) the identification of the applicant for business;

(b) the verification of the identity of the applicant for business using reliable, independent source documents, data or information;

(c) the obtaining of information on the purpose and intended nature of the business relationship;

(d) the taking of reasonable steps to establish the source of funds;

(e) ensure sub-paragraphs (a) to (d) are carried out in accordance with paragraph 5.

(4) Sub-paragraph (1) shall not require verification of identity to be produced if —

(a) the identity of the applicant for business is known to the relevant person;

(b) the relevant person knows the nature and intended purpose of the relationship; and

(c) the relevant person has satisfied itself that the applicant for business is a person listed in sub-paragraph (5).

(5) The persons referred to in sub-paragraph (4)(c) are —

(a) a regulated person;

(b) an advocate within the meaning of the Advocates Act 1976, a registered legal practitioner within the meaning of the Legal Practitioners Registration Act 1986[15] or an accountant carrying out business in or from the Isle of Man, where the relevant person is satisfied that the rules of the professional body of the

[15] 1986 c.15

applicant for business embody requirements and procedures that are at least equivalent to this Code; or

(c) a person who acts in the course of external regulated business and is regulated under the law and regulations of a country that is included in the list in Schedule 2.

(6) Where the relevant person deals with an applicant for business otherwise than face-to-face, it must, in taking any steps under this paragraph, take adequate measures to compensate for any risk arising as a result.

(7) Sub-paragraph (4) shall not have effect in respect of a person mentioned in sub-paragraph (5)(c) if the relevant person has reason to believe that the country in question does not apply, or insufficiently applies, the FATF Recommendations in respect of the business of that person.

(8) Sub-paragraph (4) shall not have effect if any one of the following occurs —

(a) the relevant person knows or suspects that the transaction is or may be related to money laundering;

(b) a suspicious pattern of behaviour that causes the relevant person to know or suspect that the behaviour is or may be related to money laundering;

(c) the relevant person becomes aware of anything which causes the relevant person to doubt the identity of the applicant for business or beneficial owner;

(d) the relevant person becomes aware of anything which causes the relevant person to doubt the *bona fides* of the applicant for business or beneficial owner.

(9) Except as provided in sub-paragraph (4), procedures comply with sub-paragraph (1) if they require that when evidence of identity in accordance with paragraph 6(3) is not obtained or produced;

(a) the business relationship and transactions shall not proceed any further; and

(b) the relevant person shall terminate that relationship; and

(c) the relevant person must consider whether a suspicious transaction report should be made.

7 Continuing business relationships

(1) A relevant person shall establish, maintain and operate the procedures specified in sub-paragraph (3).

(2) Those procedures shall be undertaken during a business relationship as soon as reasonably practicable after any one of the following occurs —

(a) a transaction that the relevant person suspects may be related to money laundering; or

(b) a suspicious pattern of behaviour that causes the relevant person to know or suspect that the behaviour is or may be related to money laundering; or

(c) transactions or patterns of transactions that are complex or unusually large and which have no apparent economic or visible lawful purpose; or

(d) unusual patterns of transactions which have no apparent economic or visible lawful purpose; or

(e) the relevant person becomes aware of anything which causes the relevant person to doubt the identity of the person who, in relation to the formation of the business relationship, was the applicant for business; or

(f) the relevant person becomes aware of anything which causes the relevant person to doubt the veracity or adequacy of evidence of identity produced under paragraph 6(3).

(3) The procedures referred to in sub-paragraph (1) are —

(a) an examination of the background and purpose of the transactions or circumstances;

(b) if no evidence of identity was produced after the business relationship was established, the taking of such steps as will require the production by the person who, in relation to the formation of the business relationship, was the applicant for business of information in accordance with paragraph 6(3);

(c) if evidence of identity was produced under paragraph 6(3), the taking of such steps as will determine whether the evidence of identity produced under that paragraph is satisfactory; or

(d) if evidence of identity produced under paragraph 6(3) is not for any reason satisfactory, the taking of such steps as will require

the production by the other party of evidence of his identity or the taking of such measures as will produce evidence of his identity in accordance with paragraph 6(3).

(4) The relevant person —

(a) shall keep written records of any examination, steps, measures or determination made or taken or under sub-paragraph (3) (which records shall be records to which paragraph 16 applies); and

(b) shall, on request, make such findings available to the competent authorities and auditors (if any).

(5) Where the relevant person deals with an applicant for business otherwise than face-to-face, it must, in taking any steps under this paragraph, take adequate measures to compensate for any risk arising as a result.

(6) Procedures comply with this paragraph if they require that when evidence of identity, in accordance with paragraph 6(3), is not obtained or produced-

(a) the business relationship and transactions shall not proceed any further; and

(b) the relevant person shall consider terminating that relationship; and

(c) the relevant person considers whether a suspicious transaction report should be made.

8 Enhanced customer due diligence

(1) Where in accordance with the risk assessment an applicant for business, poses a higher risk, the relevant person must carry out enhanced customer due diligence.

(2) For the purpose of this paragraph matters which may pose a higher risk include but are not restricted to —

(a) a business relationship or one-off transaction with —

(i) a politically exposed person; or

(ii) a person or legal arrangement resident or located in a country which the relevant person has reason to believe does

not apply, or insufficiently applies, the FATF Recommendations in respect of the business or transaction in question;

(b) a person or legal arrangement which is the subject of a warning issued by a competent authority ;

(c) a company which has shares in bearer form.

(3) In this paragraph "enhanced customer due diligence" means steps, additional to the measures specified in paragraphs 5 to 7 and 9 to 11 of the Code, for the purpose of identifying customers and other persons, namely —

(a) considering whether additional identification data needs to be obtained;

(b) considering whether additional aspects of the customer's identity need to be verified;

(c) the taking of reasonable steps to establish the source of the wealth of the customer and any beneficial owner; and

(d) considering what ongoing monitoring should be carried on in accordance with paragraph 15.

9 One-off transactions

(1) A relevant person shall establish, maintain and operate the procedures specified in sub-paragraph (3).

(2) Those procedures shall be undertaken before a one-off transaction is entered into.

(3) The procedures referred to in sub-paragraph (1) are the production by the applicant for business of —

(a) the identification of the applicant for business;

(b) the verification of the identity of the applicant for business using reliable, independent source documents, data or information;

(c) the obtaining of information on the purpose and intended nature of the one-off transaction;

(d) taking reasonable steps to establish the source of funds; and

(e) ensure sub-paragraphs (a) to (d) are carried out in accordance with paragraph 5.

(4) Sub-paragraph (1) shall not require verification of identity to be produced if the identity of the applicant for business is known to the relevant person, the relevant person knows the nature and intended purpose of the relationship and the relevant person has satisfied itself that —

(a) the applicant for business is —

(i) a regulated person;

(ii) an advocate within the meaning of the Advocates Act 1976, a registered legal practitioner within the meaning of the Legal Practitioners Registration Act 1986[16] or an accountant carrying out business in or from the Isle of Man, where the relevant person is satisfied that the rules of the professional body of the applicant for business embody requirements and procedures that are at least equivalent to this Code; or

(iii) a person who acts in the course of external regulated business and is regulated under the law and regulation of a country that is included in the list in Schedule 2; or

(b) the transaction is an exempted one-off transaction.

(5) Where the relevant person deals with an applicant for business otherwise than face-to-face, it must, in taking any steps under this paragraph, take adequate measures to compensate for any risk arising as a result.

(6) Where the one-off transaction is complex or unusually large, and has no apparent economic or visible lawful purpose, the relevant person shall take adequate measures to compensate for any risk arising as a result

(7) Sub-paragraph (4) shall not have effect in respect of a person who acts in the course of external regulated business and is based or incorporated in or formed under the law of a country that is included in the list in Schedule 2 if the relevant person has reason to believe that the country in question does not apply, or insufficiently applies, the FATF Recommendations in respect of the business of that person.

(8) Sub-paragraph (4) shall not have effect if any one of the following occurs —

[16] 1986 c.15

(a) the relevant person knows or suspects that the transaction may be, related to money laundering;

(b) a suspicious pattern of behaviour that causes the relevant person to know or suspect that the behaviour is or may be related to money laundering;

(c) the relevant person becomes aware of anything which causes the relevant person to doubt the identity of the applicant for business or beneficial owner;

(d) the relevant person becomes aware of anything which causes the relevant person to doubt the *bona fides* of the applicant for business or beneficial owner;

(e) where the provisions of sub paragraph (6) apply.

(9) Except as provided in sub-paragraph (4), procedures comply with sub-paragraph (1) if they require that when evidence of identity in accordance with paragraph 6(3) is not obtained or produced;

(a) no one-off transactions shall be carried out ; and

(b) the relevant person must consider whether a suspicious transaction report should be made.

10 Politically Exposed Persons

(1) A relevant person must maintain appropriate procedures and controls for the purpose of determining whether any of the following is a politically exposed person —

(a) an applicant for business;

(b) a customer;

(c) any natural person having power to direct the activities of a person mentioned in sub-paragraph (a) or (b);

(d) the beneficial owner of a person mentioned in sub-paragraph (a) or (b);

(e) a known beneficiary of a legal arrangement mentioned in sub-paragraph (a) or (b).

(2) A relevant person must maintain appropriate procedures and controls for requiring the approval of its senior management —

(a) before any business relationship is established with a politically exposed person; or

(b) before any one-off transaction is carried out with a politically exposed person; or

(c) where it is discovered that an existing business relationship is with a politically exposed person, to the continuance of that relationship.

11 Introduced business

(1) Where an applicant for business is introduced to a relevant person by a third party (in this paragraph referred to as "the introducer"), the relevant person may, if that person thinks fit, choose to comply with the provisions of this paragraph, instead of the provisions of paragraphs 6 or 9.

(2) The relevant person shall establish, maintain and operate the procedures specified in sub-paragraph (4).

(3) Those procedures shall be undertaken before a business relationship is entered into.

(4) The procedures referred to in sub-paragraph (1) are —

(a) the production by the introducer of evidence of the identity of the applicant for business in accordance with paragraph 6(3); or

(b) the taking of such other measures as will produce evidence of their identity in accordance with paragraph 6(3).

(5) Sub-paragraph (1) shall not require verification of identity to be produced if —

(a) the relevant person has identified the applicant for business and the beneficial owner;

(b) the relevant person knows the nature and intended purpose of the relationship; and

(c) the relevant person has satisfied itself that —

(i) the introducer is —

(A) a regulated person; or

(B) an advocate, a registered legal practitioner within the meaning of the Legal Practitioners Registration Act 1986 or an accountant carrying out business in or from the Isle of Man, where the relevant person is satisfied that the rules of the professional body of the introducer embody requirements and procedures that are at least equivalent to this Code;

(ii) the relevant person and the applicant for business are bodies corporate in the same group; or

(iii) the transaction is an exempted one off transaction; or

(iv) the introducer acts in the course of an external regulated business and is regulated under the law and regulations of a country that is included in the list in Schedule 2.

(6) Sub-paragraph (5)(c)(iv) shall not have effect in any case where the relevant person has reason to believe that the country in question does not apply, or insufficiently applies, the FATF Recommendations in respect of the business of the introducer.

(7) The relevant person shall not enter into a business relationship with a person that is introduced by an introducer unless written terms of business are in place between the relevant person and the introducer, and those terms of business, notwithstanding sub-paragraph (3) and (4), in all cases require the introducer to —

(a) verify the identity of all applicants for business introduced to the relevant person sufficiently to comply with the money laundering requirements;

(b) verify the identity of the beneficial owner;

(c) establish and maintain a record of the evidence of identity for at least 5 years calculated in accordance with paragraph 17(1);

(d) establish and maintain records of all transactions between —

(i) the introducer and the applicant for business;

(ii) the relevant person and the introducer; and

(iii) the relevant person and the applicant for business if the introducer has received copies of records relating to those transactions,

if the records are concerned with or arise out of the introduction (whether directly or indirectly) for at least 5 years calculated in accordance with paragraph 17(1);

(e) supply to the relevant person forthwith upon request, copies of the evidence verifying the identity of the applicant for business and the beneficial owner and all other customer due diligence data held by the introducer in any particular case;

(f) supply to the relevant person forthwith copies of the evidence verifying the identity of the applicant for business and the beneficial owner and all other customer due diligence data, in accordance with paragraph 6(3), held by the introducer in any particular case where —

(i) the introducer is to cease trading;

(ii) the introducer is to cease doing business with the applicant for business;

(iii) where the relevant person informs the introducer that it no longer intends to rely on the terms of the terms of business entered into under the provisions of this paragraph;

(g) inform the relevant person specifically of each case where the introducer is not required or has been unable to verify the identity of the applicant for business or the beneficial owner;

(h) inform the relevant person where the introducer is no longer able to comply with the provisions of the written terms of business because of a change of the law applicable to the introducer; and

(i) do all such things as may be required by the relevant person to enable the relevant person to comply with its obligation under sub-paragraph (9).

(8) It is the responsibility of the relevant person to ensure that the procedures under sub-paragraph (4) are fit for the purpose of ensuring that the evidence produced or to be produced is satisfactory and that the procedures of the introducer are likewise fit for that purpose.

(9) A relevant person shall take steps to satisfy itself that the procedures for implementing this paragraph are effective by testing them on a random and periodic basis and the written terms of business shall confer the necessary rights on the relevant person.

(10) A relevant person shall take steps to satisfy itself that the introducer is a person as described by sub-paragraph 5(c) and take such steps as necessary to ensure

he becomes aware of any material change to the introducers status or the status of the jurisdiction in which the introducer is regulated.

(11) Sub-paragraph (5) shall not have effect if any one of the following occurs —

(a) the relevant person knows or suspects that the transaction is or may be related to money laundering;

(b) a suspicious pattern of behaviour that causes the relevant person to know or suspect that the behaviour is or may be related to money laundering;

(c) the relevant person becomes aware of anything which causes the relevant person to doubt the identity of the applicant for business or the introducer or beneficial owner;

(d) the relevant person becomes aware of anything which causes the relevant person to doubt the *bona fides* of the applicant for business or the introducer or beneficial owner.

(12) Except as provided in sub-paragraph (5), procedures comply with this paragraph if they require that when evidence of identity, in accordance with paragraph 6(3), is not obtained or produced —

(a) the business relationship and transactions shall not proceed any further; and

(b) the relevant person shall terminate that relationship; and

(c) the relevant person must consider whether a suspicious transaction report should be made.

(13) The ultimate responsibility for ensuring that customer due diligence procedures comply with the terms of this Code remains with the relevant person.

(14) In sub-paragraph (5)(c)(ii), "group", in relation to a body corporate, means that body corporate, any other body corporate which is its holding company or subsidiary and any other body corporate which is a subsidiary of that holding company, and "subsidiary" and "holding company" shall be construed in accordance with section 1 of the Companies Act 1974[17].

[17] 1974 c.30

12 Exceptions from customer due diligence procedures

(1) An insurer need not comply with paragraphs 5 to 11 where —

(a) a premium is an exempted one off transaction; or

(b) a policy has neither a surrender value nor a maturity value (for example, term insurance).

(2) In respect of sub-paragraph (1) having paid due regard to the money laundering risk, an insurer may consider it appropriate —

(a) to comply immediately with the requirements of the Code referred to in those paragraphs; or

(b) to comply with the requirements of the Code referred to in those paragraphs, but to defer compliance until a claim is made or the policy is cancelled.

(3) Where a claim is made on a policy with neither a surrender value nor a maturity value (for example on the occurrence of an event), and the amount of the settlement is greater than that set out in sub-paragraph (1)(a) the insurer must satisfy itself as to the identity of the policyholder or claimant (if not the policyholder).

(4) Where a policy is cancelled resulting in the repayment of premium(s) and the amount of the settlement is greater than that set out in sub-paragraphs (1)(a) the insurer must satisfy itself as to the identity of the applicant or claimant (if different to the policyholder) and must also ensure it is satisfied as to the original source of wealth and source of funds.

(5) An insurer need not comply with sub-paragraph (3) where settlement of the claim is to—

(a) a third party in payment for services provided (for example to a hospital where health treatment has been provided);

(b) a supplier for services or goods; or

(c) the policyholder(s) where invoices for services or goods have been provided to the insurer,

and the insurer believes the services or goods to have been supplied.

13 Correspondent banking services

(1) This paragraph applies to a business relationship or one-off transaction, as the case may be, which involves correspondent banking services or similar arrangements.

(2) A relevant person must not enter into or continue a relationship to which this paragraph applies with a shell bank.

(3) A relevant person must not enter into or continue a relationship to which this paragraph applies with a financial institution in a country or territory outside the Island unless it is satisfied that the respondent bank does not permit its accounts to be used by shell banks.

(4) Before entering into a relationship or transaction to which this paragraph applies, a relevant person must take the following additional steps —

(a) obtain sufficient information about the respondent bank to understand fully the nature of its business;

(b) determine from publicly available information —

(i) the reputation of the respondent bank;

(ii) the quality of the supervision to which it is subject; and

(iii) whether it has been subject to investigation or regulatory action with respect to money laundering or the financing of terrorism;

(c) assess the procedures and controls maintained by the respondent bank for preventing money laundering or the financing of terrorism, and ascertain that they are adequate and effective;

(d) ensure that the approval of the relevant person's senior management is obtained; and

(e) document the respective responsibilities of the relevant person and the respondent bank with respect to measures to prevent money laundering and the financing of terrorism.

(5) Where a relationship or transaction to which this paragraph applies involves a payable-through account, a relevant person must be satisfied that the respondent bank —

(a) has taken steps complying with the requirements of Recommendation 5 (customer due diligence and record keeping) of the FATF Recommendations with respect to every customer having direct access to the account; and

(b) will provide the relevant person on request with relevant evidence of the identity of the customer.

14 Foreign branches and subsidiaries

(1) A relevant person must ensure that any branch or subsidiary in a country outside the Island takes measures consistent with this Code, and guidance issued by a competent authority for preventing money laundering and the financing of terrorism, to the extent permitted by the laws and regulations of that country .

(2) Where the minimum measures for preventing money laundering and the financing of terrorism in such a country differ from those required by the law of the Island, the relevant person must ensure that any branch or subsidiary in that country applies the higher standard, to the extent permitted by the laws and regulations of that country.

(3) The relevant person must inform the competent authority when a branch or subsidiary is unable to take any of the measures referred to in sub-paragraph (1) or (2) because it is prohibited by the laws and regulations of the country concerned.

(4) In this paragraph "subsidiary", in relation to a relevant person, means a legal person more than half of whose equity share capital is owned by the relevant person.

15 Ongoing monitoring

(1) A relevant person must perform ongoing and effective monitoring of any existing business relationship, including —

(a) review of information held for the purpose of customer due diligence to ensure that it is up to date and appropriate (in particular where the relationship poses a higher risk);

(b) appropriate scrutiny of transactions and other activities, paying particular attention to transactions which are —

(i) complex;

(ii) both large and unusual; or

(iii) of an unusual pattern,

and which have no apparent economic or lawful purpose; and

(c) appropriate scrutiny of transactions to ensure that they are consistent with the relevant person's knowledge of the customer, its business and risk profile and, where necessary, the source of funds.

(2) The extent and frequency of any monitoring under this paragraph must be determined in accordance with paragraph 3(4)

(3) Where the relevant person deals with a customer otherwise than face-to-face, it must, in carrying out any monitoring under this paragraph, take adequate measures to compensate for any risk arising as a result.

RECORD KEEPING

16 Records

A relevant person must keep the records specified in this paragraph —

(a) a copy of the evidence of identity obtained or information that enables a copy of such evidence to be obtained pursuant to paragraphs 5 to 14;

(b) a record of all transactions carried out in the course of relevant business, including identification data, account files and business correspondence records ; and

(c) such other records as are sufficient to permit reconstruction of individual transactions and compliance with this Code.

17 Retention of records

(1) A relevant person shall keep the records required by this Code for at least 5 years from —

(a) in the case of records required by paragraph 16(b), the date of the completion of the transaction;

(b) in other cases, from the date when —

(i) all activities relating to a one-off transaction or a series of linked transactions were completed; or

(ii) in respect of other activities —

(A) the business relationship was formally ended; or

(B) if the business relationship was not formally ended, when all activities relating to the transaction were completed.

(2) Where a report has been made to a constable in pursuance of paragraph 20(2)(f), or the person knows or believes that a matter is under investigation, that person shall, without prejudice to sub-paragraph (1), retain all relevant records for as long as required by the constable.

(3) Where the relevant person becomes aware that a request for information or an enquiry is underway by a competent authority, that person shall, without prejudice to sub-paragraph (1), retain all relevant records for as long as required by the competent authority.

18 Format and retrieval of records

(1) A relevant person shall ensure that any records required to be established and maintained under this Code —

(a) if the records are in the form of hard copies kept in the Island, ensure that they are capable of retrieval without undue delay;

(b) if the records are in the form of hard copies kept outside the Island, ensure that the copies can be sent to the Island and made available within 7 working days; and

(c) in the case of other records (e.g. copies kept on a computer system), ensure that they are readily accessible in or from the Island and that they are capable of retrieval without undue delay.

(2) A relevant person may rely on the records of a third party in respect of the details of payments and transactions by customers, provided that it is satisfied that —

(a) the third party is required upon request to produce copies of the records required;

(b) the third party must notify the relevant person that they are no longer able to comply with sub-paragraph (a) for whatever reason

19 Register of money laundering enquiries

(1) A relevant person shall establish and maintain a register of all enquiries made of it by law enforcement or other authorities acting under powers provided by the money laundering requirements.

(2) The register established and maintained under sub-paragraph (1) shall be kept separate from other records and shall contain as a minimum the date and nature of the enquiry, the name and agency of the inquiring officer, the powers being exercised, and details of the accounts or transactions involved.

20 Recognition and reporting of suspicious transactions

(1) A relevant person shall appoint a Money Laundering Reporting Officer to exercise the functions conferred on him by this paragraph and the MLRO —

(a) must be —

(i) sufficiently senior in the organisation of the relevant person; or

(ii) if not within that organisation, have sufficient experience and authority; and

(b) must have a right of direct access to the directors, the managing board or the partners (as the case may be) of the relevant person,

to be effective in the exercise of his or her functions.

(2) A relevant person shall establish, maintain and operate written internal reporting procedures which, in relation to its relevant business, will —

(a) enable all its directors or, as the case may be, partners, all other persons involved in its management, and all appropriate employees to know to whom they should report any knowledge or suspicions of money laundering activity;

(b) ensure that there is a clear reporting chain under which those suspicions will be passed to the MLRO;

(c) require reports to be made to the MLRO of any information or other matter which comes to the attention of the person handling that business and which in that person's opinion gives rise to a knowledge or suspicion that another person is engaged in money laundering;

(d) require the MLRO to consider any report in the light of all other relevant information available to him for the purpose of determining whether or not it gives rise to a knowledge or suspicion of money laundering;

(e) ensure that the MLRO has full access to any other information which may be of assistance to him and which is available to the relevant person; and

(f) enable the information or other matter contained in a report to be disclosed promptly to a constable who is for the time being serving with the organisation known as the Financial Crime Unit where the MLRO knows or suspects that another is engaged in money laundering.

(3) A relevant person shall establish and maintain a register of all reports made to a constable in pursuance of sub-paragraph (2)(f).

(4) The register established and maintained under sub-paragraph (3) shall contain details of the date on which the report is made, the person who makes the report, the constable to whom it is made and information sufficient to identify the relevant papers.

STAFF, TRAINING AND TECHNOLOGICAL DEVELOPMENTS

21 Staff, etc. screening

A relevant person shall establish, maintain and operate appropriate procedures to enable the relevant person to satisfy itself of the integrity of new directors or partners (as the case may be) of the relevant person and of all new appropriate employees.

22 Staff training: money laundering requirements

A relevant person shall provide or cause to be provided education and training including refresher training (not less than annually) for all directors or, as the case may be, partners, all other persons involved in its management, all key staff and appropriate employees to ensure that they are aware of —

(a) the provisions of the money laundering requirements;

(b) their personal obligations under the money laundering requirements;

(c) the internal reporting procedures established under paragraph 20;

(d) the relevant person's policies and procedures to prevent money laundering;

(e) the relevant person's customer identification, record-keeping and other procedures;

(f) the recognition and handling of suspicious transactions;

(g) their personal liability for failure to report information or suspicions in accordance with internal procedures; and

(h) new developments, including information on current techniques, methods and trends in money laundering and the financing of terrorism.

23 Technological developments

A relevant person must maintain appropriate procedures and controls for the purpose of preventing the misuse of technological developments for the purpose of money laundering or the financing of terrorism.

Made 2008

_____

Minister for Home Affairs

SCHEDULES

Paragraph 2

SCHEDULE 1

RELEVANT BUSINESS

1. Business carried on by a building society within the meaning of section 7 of the Industrial and Building Societies Act 1892.

2. Business carried on by a society (other than a building society or credit union) registered under the Industrial and Building Societies Act 1892.

3. Any activity carried on for the purpose of raising money authorised to be borrowed under the Isle of Man Loans Act 1974[18].

4. The business of an estate agent within the meaning of the Estate Agents Act 1975[19].

5. The provision by way of business of audit services in respect of a body corporate.

6. (1) Any activity specified in sub-paragraph (2) that is undertaken by —

   (a) an advocate within the meaning of the Advocates Act 1976;

   (b) a registered legal practitioner within the meaning of the Legal Practitioners Registration Act 1986;

   (c) a Notary Public within the meaning of the Advocates Act 1995 and the Notaries Regulations 2000;

   (d) an accountant or a person who, in the course of business, provides accountancy services,

   (2) The activities referred to in sub-paragraph (1) are —

   (a) holding or managing any assets belonging to a client;

   (b) the provision of legal services which involves participation in a financial or real property transaction (whether by assisting in the planning or execution of any such transaction or otherwise) by acting for, or on behalf of, a client in respect of —

   (i) the sale or purchase of land;

   (ii) managing bank, savings or security accounts;

   (iii) organising contributions for the promotion, formation, operation or management of bodies corporate;

   (iv) the sale or purchase of a business;

[18] 1974 c.6
[19] 1975 c.6

(v) the creation, operation or management of a legal structure or legal arrangement.

7. Insurance business within the meaning of the Insurance Act 2008.

8. The business of acting as an insurance manager for or in relation to an insurer within the meaning of the Insurance Act 2008.

9. Any activity permitted to be carried on by a licence holder under a casino licence granted under the Casino Act 1986[20].

10. A collective investment scheme within the meaning of section 1 of the Collective Investment Schemes Act 2008 notwithstanding the provisions of the Collective Investment Scheme (Definition) Order 2008 had not been made[21].

11. The business of a bookmaker within the meaning of the Gaming, Betting and Lotteries Act 1988[22] but excluding activities to which the Anti-Money Laundering (Online Gambling and Peer to Peer Gambling) Code 2006[23] applies.

12. Investment business within the meaning of section 3 of the Financial Services Act 2008 and Class 2 of Schedule 1 to the Regulated Activities Order 2008 as if the exclusions contained within the Order or the Financial Services (Exemptions) Regulations 2008 had not been made.

13. Business carried by a society registered as a credit union within the meaning of the Credit Unions Act 1993[24].

14. The business of insurance intermediary within the meaning of the Insurance Act 2008

15. Deposit taking within the meaning of section 3 of the Financial Services Act 2008 and Class 1 of Schedule 1 to the Regulated Activities Order 2008 ignoring any exclusions for that class contained within the Order or the Financial Services (Exemptions) Regulations 2008 had not been made.

16. Corporate services or trust services within the meaning of section 3 of the Financial Services Act 2008 and Classes 4 and 5 of Schedule 1 to the Regulated Activities Order 2008 ignoring any exclusions for that class contained within the Order or the Financial Services (Exemptions) Regulations 2008.

17. Acting as a retirement benefits schemes administrator within the meaning of Part 6 of the Retirement Benefits Schemes Act 2000.

18. Acting as the trustee of a retirement benefits scheme within the meaning of the Retirement Benefits Schemes Act 2000.

[20] 1986 c.16
[21] 1988 c.16
[22] 1988 c.17
[23] SD 782/06
[24] 1993 c.19

19. Any activity carried on for the purpose of raising money by a local authority.

20. The business of a *bureau de change*.

21. The business of the Post Office in respect of any activity undertaken on behalf of the National Savings Bank.

22. Any activity involving money (including any representation of monetary value) transmission services or cheque encashment facilities.

23. The provision of safe custody facilities for cash or liquid securities on behalf of other persons.

24. The business of dealing in goods of any description (including dealing as an auctioneer) whenever a transaction involves accepting a total cash payment of euro 15,000 or more.

25. Subject to note 2 below, lending including, but not limited to, consumer credit, mortgage credit factoring and the finance of commercial transactions.

26. Subject to note 2 below, financial leasing arrangements in respect of products other than consumer products.

27. Any business involving the issuing and managing of means of payment (including but not limited to credit and debit cards, cheques, traveller's cheques, money orders, bankers' drafts and electronic money).

28. Subject to note 2 below, the business of providing financial guarantees and commitments.

29. Administering or managing money on behalf of other persons.

30. Services to collective investment schemes as defined in section 3 of the Financial Services Act 2008 and Class 3 of Schedule 1 to the Regulated Activities Order 2008 ignoring any exclusions for that class contained within the Order or the Financial Services (Exemptions) Regulations 2008.

Note 1. Paragraphs 25 to 30 are additional to paragraphs 1 to 24.

Note 2. A person does not carry on relevant business by reason only of the provisions of paragraphs 25, 26 or 28 of this Schedule if the lending, leasing or provision of guarantees or commitments (as the case may be) is made by:-

(a) a parent undertaking to a subsidiary of that parent undertaking;

(b) a subsidiary of a parent undertaking to the parent undertaking; or

(c) a subsidiary of a parent undertaking to another subsidiary of that parent undertaking.

Note 3. In Note 2 "parent undertaking" means an undertaking which, in relation to another undertaking, a "subsidiary":-

(a) owns or controls, whether directly or indirectly, shares or other interests in the subsidiary together aggregating in excess of 50 per cent of the votes exercisable at general or other meetings of the subsidiary on any or all matters;

(b) has a right to appoint or remove a majority of its board of directors, or other governing body;

(c) has the right to exercise a dominant influence over the subsidiary:-

(i) by virtue of the provisions contained in the subsidiary's constitutional documents, or

(ii) by virtue of a control contract; or

(d) controls, alone or pursuant to an agreement with other persons, a majority of the voting rights in the subsidiary; and

"undertaking" means a natural person, body corporate, trust, partnership or unincorporated association.

Note 4. For the purposes of Note 3:-

(a) an undertaking is taken to have the right to exercise a dominant influence over another undertaking only if it has a right to give directions with respect to the operating and financial policies of that other undertaking with which its directors are, or governing body is, obliged to comply whether or not they are for the benefit of that other undertaking;

(b) "control contract" means a contract in writing conferring a dominant influence right which:-

(i) is of a kind authorised by the constitutional documents of the undertaking in relating to which the right is exercisable; and

(ii) is permitted by the law under which that undertaking is established; and

(c) any undertaking which is a subsidiary of another undertaking is also a subsidiary of any further undertaking of which that other is a subsidiary."

Paragraphs 6, 9 and 11

SCHEDULE 2

LIST OF COUNTRIES

Argentina
Australia
Austria
Belgium
Bermuda
Brazil
Canada
Cayman Islands
Cyprus
Denmark
Finland
France
Germany
Gibraltar
Greece
Guernsey
Hong Kong
Iceland
Ireland
Italy
Japan
Jersey
Luxembourg
Malta
Mauritius
Monaco
Netherlands
New Zealand
Norway
Portugal
Singapore
South Africa
Spain
Sweden
Switzerland
United Kingdom
United States of America

Explanatory Note

(This note is not part of the Code)

The Criminal Justice (Money Laundering) Code 2008 is made under section 17F of the Criminal Justice Act 1990 and revokes and replaces the Anti-Money Laundering Code 2007 (SD 712/07), as amended by SD 903/07 and SD 296/07. The Code contains anti-money laundering provisions in line with Financial Action Task Force's Recommendations on money laundering and terrorist financing and accompanying methodology.

Financial Services Rule Book 2008

PART 9 — MONEY-LAUNDERING AND FINANCING OF TERRORISM

9.1 Application

This Part applies to all licenceholders.

9.2 Interpretation

(1) In this Part —

"beneficial owner" means the natural person who ultimately owns or controls an applicant for business or on whose behalf a transaction or activity is being conducted; and in relation to a legal person or legal arrangement, 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 (whether through direct or indirect ownership or control, including through bearer share holdings) more than 25% of the shares or voting rights in the legal person; or

(b) in the case of any legal person, a natural person who otherwise exercises control over the management of the legal person;

(c) in the case of a legal arrangement —

(i) the trustees or other persons controlling the applicant; and
(ii) the settlor or other person by whom the arrangement is made,

"the Code" means the Criminal Justice (Money Laundering) Code 2007;

"correspondent banking services" means banking services provided by a financial institution in one country or territory ("the correspondent bank") to a financial institution in another country or territory ("the respondent bank");

"customer due diligence" (except in the expression "enhanced customer due diligence") means the measures specified in paragraphs 5 to 8 of the Code;

"legal arrangement" means —

(a) an express trust, or
(b) any other arrangement which has a similar legal effect (such as a *fiducie, Treuhand* or *fideicomiso*);

"legal person" includes any body corporate or unincorporate which is capable of establishing a permanent customer relationship with a financial institution or of owning property;

"money laundering reporting officer" means an individual appointed under paragraph 14(1) of the Code;

"payable-through account" means an account maintained by a correspondent bank which may be operated directly by a customer of the respondent bank;

"politically exposed person" means any of the following resident in a country or territory outside the Island —

(a) a natural person who is or has been entrusted with prominent public functions, including —

(i) a head of state, head of government, minister or deputy or assistant minister;

(ii) a senior government official;

(ii) a member of parliament;

(iv) a senior politician;

(v) an important political party official;

(vi) a senior judicial official;

(vii) a member of a court of auditors or the board of a central bank;

(viii) an ambassador, chargé d'affaires or other high-ranking officer in a diplomatic service;

(ix) a high-ranking officer in an armed force;

(x) a senior member of an administrative, management or supervisory body of a State-owned enterprise; and

(xi) a senior official of an international entity or organisation;

(b) any of the following family members of a person mentioned in subparagraph (a) —

(e) a spouse;

(iii) a partner considered by national law as equivalent to a spouse;

(iv) a child or the spouse or partner of a child;

(iv) a brother or sister (including a half-brother or half-sister);

(v) a parent;

(vi) a parent-in-law;

(vii) a grandparent; and

(viii) a grandchild;

(c) any close associate of a person mentioned in sub-paragraph (a), including —

(i) any natural person who is known to have joint beneficial ownership of a legal entity or legal arrangement, or any other close business relations, with such a person;

(ii) any natural person who has sole beneficial ownership of a legal entity or legal arrangement which is known to have been set up for the benefit of such a person;

(iii) any natural person who is known to be beneficiary of a legal arrangement of which such a person is a beneficial owner or beneficiary;

(v) any natural person who is in a position to conduct substantial financial transactions on behalf of such a person.

"risk" means a risk of money laundering or the financing of terrorism, or both;

(2) In this Part “shell bank” means a bank which is —

(a) incorporated in a country or territory in which it has no physical presence, and

(b) not affiliated with a financial services group which is subject to effective consolidated supervision;

and for this purpose —

"consolidated supervision", in relation to a financial services group, means supervision of the group by a regulatory body on the basis of the totality of its business, wherever conducted;

"financial services group" means a group of companies whose activities include to a significant extent activities which are, or if carried on in the Island would be, regulated activities.

(3) In this Part the following expressions have the same meanings as in the Code —

"applicant for business"
"business relationship"
"FATF Recommendations"
"one-off transaction"

9.3 Anonymous accounts etc.

(1) A licenceholder must not maintain —

(a) an anonymous account, or

(b) an account in a fictitious name.

(2) If a licenceholder maintains a numbered account it must —

(a) identify, and verify the identity of, the customer, and

(b) maintain the account in such a way as to comply fully with the requirements of the Code and this Part.

9.4 Business risk assessment

(1) For the purpose of determining the measures to be taken when carrying out customer due diligence, a licenceholder must carry out a risk assessment in accordance with this rule.

(2) The assessment must estimate the risk of money laundering and terrorist financing on the part of the licenceholder's customers, having regard to —

(a) the nature, scale and complexity of its activities;

(b) the products and services provided by it, and

(c) the persons to whom, and the manner in which, they are provided.

(3) The assessment must be —

(a) undertaken as soon as reasonably practicable —

(i) after this Part comes into force, in the case of an existing business;

(ii) after the licenceholder commences business, in any other case; and

(b) regularly reviewed and, where appropriate, amended so as to keep it up to date.

9.5 Customer due diligence — general

When carrying out customer due diligence, whether in relation to an applicant for business, an existing business relationship or a one-off transaction, a licenceholder must do so —

(a) on the basis of materiality and risk, and

(b) in accordance with its current risk assessment under rule 9.4.

9.6 Customer due diligence procedures

(1) This rule applies where a licenceholder is operating the procedures required by paragraphs 5 to 8 of the Code, except where paragraph 5(4) or 7(4) of the Code applies.

(2) The licenceholder must, in the case of any applicant for business, —

(a) determine who is the beneficial owner of the applicant;

(b) take reasonable steps to verify the identity of those persons, using relevant information or data obtained from a reliable source; and

(c) determine whether the applicant is acting on behalf of another person and, if so, take reasonable steps to identify that other person, and to verify his identity using relevant information or data obtained from a reliable source.

(3) Without prejudice to paragraph (2), the licenceholder must, in the case of an applicant for business which is a legal person or legal arrangement —

(a) verify that any person purporting to act on behalf of the applicant is authorised to do so;

(b) identify and verify the identity of that person using reliable and independent source documents, data or information;

(c) in the case of a legal arrangement, identify any known beneficiaries;

(d) verify the legal status of the applicant using relevant information or data obtained from a reliable source;

(e) obtain information concerning the names and addresses of the applicant and any natural persons having power to direct its activities;

(f) obtain information concerning the person by whom, and the method by which, binding obligations may be imposed on the applicant;

(g) take reasonable steps to understand the ownership and control structure of the applicant.

(4) Where the licenceholder deals with an applicant for business otherwise than face-to-face, it must, in taking any steps under this rule, take adequate measures to compensate for any risk arising as a result.

(5) The licenceholder must not proceed with the business relationship or transaction in question unless the requirements of paragraph (2) and (where appropriate) paragraphs (3) and (4) have been complied with.

(6) In this rule "applicant for business", in relation to a continuing business relationship, means the person who, in relation to the formation of the business relationship, was the applicant for business.

9.7 Source of funds

(1) This rule applies where —

(a) a licenceholder enters into a new business relationship with a customer,

(b) in the course of a continuing business relationship between the licenceholder and a customer, any of the events referred to in paragraph 6(2) of the Code occurs, or

(c) the licenceholder enters into a one-off transaction with or on behalf of a customer.

(2) The licenceholder must take all reasonable steps to establish the source of the customer's funds with which the relationship or transaction is concerned.

9.8 Payments to beneficiaries

A licenceholder must not make a payment of income or capital under a legal arrangement to a beneficiary of the arrangement unless it has —

(a) identified the beneficiary, and

(b) verified his identity using relevant information or data obtained from a reliable source.

9.9 Enhanced customer due diligence

(1) Where in accordance with the risk assessment an applicant for business, business relationship or one-off transaction poses a higher risk, the licenceholder must carry out enhanced customer due diligence.

(2) For the purpose of this rule matters which pose a higher risk include but are not restricted to —

(a) a business relationship or one-off transaction with —

(i) a politically exposed person; or

(ii) a person or legal arrangement resident or located in a country which the licenceholder has reason to believe does not apply, or insufficiently applies, the FATF Recommendations in respect of the business or transaction in question;

(b) a person or legal arrangement which is the subject of a warning issued by the Commission for the purpose of this rule; and

(c) a company which has shares in bearer form.

(3) In this rule "enhanced customer due diligence" means steps, additional to the measures specified in paragraphs 5 to 8 of the Code, for the purpose of identifying customers and other persons, namely —

(a) considering whether additional identification data needs to be obtained;

(b) considering whether additional aspects of the customer's identity need to be verified;

(c) taking reasonable measures to establish the source of the wealth of the customer and any beneficial owner; and

(d) considering what ongoing monitoring should be carried on in accordance with rule 9.15.

9.10 Introduced business

(1) This rule applies where a licenceholder enters into a business relationship with a person ("the customer") who is introduced by a third party ("the introducer").

(2) The written terms of business between the licenceholder and the introducer which are required by sub-paragraph (6) of paragraph 8 of the Code must, in addition to the requirements specified in that sub-paragraph, include that mentioned in paragraph (3).

(3) The requirement referred to in paragraph (2) is that, if the introducer at any time is no longer able to comply with those requirements, whether —

(i) because of a change in the law applicable to the introducer, or in the terms of business between the introducer and the customer;

(ii) because the introducer has ceased to do business with the customer, or has ceased trading; or

(iii) for any other reason;

the introducer must —

(a) notify the licenceholder that he is no longer able to comply, and

(b) provide the licenceholder with the records, or copies of the records, which the introducer maintains pursuant to that sub-paragraph.

9.11 Politically exposed persons

(1) A licenceholder must maintain appropriate procedures and controls for the purpose of determining whether any of the following is a politically exposed person —

(a) an applicant for business;

(b) a customer;

(c) any natural person having power to direct the activities of a person mentioned in sub-paragraph (a) or (b);

(d) the beneficial owner of a person mentioned in sub-paragraph (a) or (b);

(e) a known beneficiary of a legal arrangement mentioned in subparagraph (a) or (b).

(2) A licenceholder must maintain appropriate procedures and controls for requiring the approval of its senior management —

(a) before any business relationship is established with a politically exposed person; or

(b) where it is discovered that an existing business relationship is with a politically exposed person, to the continuance of that relationship.

9.12 Correspondent banking services

(1) This rule applies to a business relationship or one-off transaction, as the case may be, which involves correspondent banking services or similar arrangements.

(2) A licenceholder must not enter into or continue a relationship to which this rule applies with a shell bank.

(3) A licenceholder must not enter into or continue a relationship to which this rule applies with a financial institution in a country or territory outside the Island unless it is satisfied that the respondent bank does not permit its accounts to be used by shell banks.

(4) Before entering into a relationship or transaction to which this rule applies, a licenceholder must take the following additional steps —

(a) obtain sufficient information about the respondent bank to understand fully the nature of its business;

(b) determine from publicly available information —

(i) the reputation of the respondent bank,

(ii) the quality of the supervision to which it is subject, and

(iii) whether it has been subject to investigation or regulatory action with respect to money laundering or the financing of terrorism;

(c) assess the procedures and controls maintained by the respondent bank for preventing money laundering or the financing of terrorism, and ascertain that they are adequate and effective;

(d) ensure that the approval of the licenceholder's senior management is obtained;

(e) document the respective responsibilities of the licenceholder and the respondent bank with respect to measures to prevent money laundering and the financing of terrorism.

(5) Where a relationship or transaction to which this rule applies involves a payable-through account, a licenceholder must be satisfied that the respondent bank —

(a) has taken steps complying with the requirements of Recommendation 5 (customer due diligence and record keeping) of the FATF Recommendations with respect to every customer having direct access to the account; and

(b) will provide the licenceholder on request with relevant evidence of the identity of the customer.

9.13 Technological developments

A licenceholder must maintain appropriate procedures and controls for the purpose of preventing the misuse of technological developments for the purpose of money laundering or the financing of terrorism.

9.14 Foreign branches and subsidiaries

(1) A licenceholder must ensure that any branch or subsidiary in a country or territory outside the Island takes measures consistent with the Code, this Rule Book and guidance issued by the Commission for preventing money laundering and the financing of terrorism, to the extent permitted by the laws and regulations of that country or territory.

(2) Where the minimum measures for preventing money laundering and the financing of terrorism in such a country or territory differ from those required by the law of the Island, the licenceholder must ensure that any branch or subsidiary in that country or territory applies the higher standard, to the extent permitted by the laws and regulations of that country or territory.

(3) The licenceholder must inform the Commission when a branch or subsidiary is unable to take any of the measures referred to in paragraph (1) or (2) because it is prohibited by the laws and regulations of the country or territory concerned.
(4) In this rule "subsidiary", in relation to a licenceholder, means a legal person more than half of whose equity share capital is owned by the licenceholder.

9.15 Ongoing monitoring

(1) A licenceholder must perform ongoing and effective monitoring of any existing business relationship, including —

(a) review of information held for the purpose of customer due diligence to ensure that it is up to date and appropriate (in particular where the relationship poses a higher risk for the purpose of rule 9.9);

(b) appropriate scrutiny of transactions and other activities, paying particular attention to transactions which are —

(i) complex,

(ii) both large and unusual, or

(iii) of an unusual pattern of transactions,

and which have no apparent economic or lawful purpose; and

(c) appropriate scrutiny of transactions to ensure that they are consistent with the licenceholder's knowledge of the customer, its business and risk profile and, where necessary, the source of funds.

(2) The extent and frequency of any monitoring under this rule must be determined —

(a) on the basis of materiality and risk,

(b) in accordance with the licenceholder's current risk assessment under rule 9.4, and

(c) having regard to whether the business relationship poses a higher risk for the purpose of rule 9.9.

(3) Where the licenceholder deals with a customer otherwise than face-to-face, it must, in carrying out any monitoring under this rule, take adequate measures to compensate for any risk arising as a result.

9.16 Retention etc. of records

(1) Where a licenceholder takes any steps under this Part for —

(a) identifying, or verifying the identity of, or obtaining any information concerning, any person, or

(b) ascertaining the source of any funds,

it must retain a record of those steps and copies of any documents produced for that purpose.

(2) The licenceholder must make the record and copies available if required to —

(a) the licenceholder's money laundering reporting officer,

(b) any other appropriate staff of the licenceholder;

(c) any constable, and

(d) the Commission.

(3) The licenceholder must keep the record and copies for at least 5 years —

(a) in the case of activities relating to a one-off transaction or a series of linked transactions, from the date when the activities were completed;

(b) in the case of activities under a business relationship —

(i) from the date when the relationship was formally ended; or

(ii) if the relationship was not formally ended, from the date when all activities relating to the transaction in question were completed.

(4) Without prejudice to paragraph (3), where —

(a) a report has been made to a constable in pursuance of paragraph 14(2)(f) of the Code, or

(b) the licenceholder knows or believes that a matter is under investigation, the licenceholder must retain all relevant records for as long as required by a constable.

Statutory Document No. 144/08

INSURANCE ACT 1986

INSURANCE (ANTI-MONEY LAUNDERING) REGULATIONS 2008

Laid before Tynwald	*15th July 2008*
Coming into operation	*1st September 2008*

In exercise of the powers conferred on the Insurance and Pensions Authority ("the Authority") by section 32 of, and Schedule 4 to, the Insurance Act 1986[1], and of all other enabling powers, and having consulted the Treasury and such other organisations and persons as appear to the Authority to be likely to be affected, the following Regulations are hereby made:—

Citation, commencement and application

1. (1) These Regulations may be cited as the Insurance (Anti-Money Laundering) Regulations 2008 and, subject to section 32(3) of the Act, shall come into operation on the 1st September 2008.

(2) These Regulations are to be followed by all insurers and, where any procedures are required to be established under these Regulations, an insurer may be asked to demonstrate compliance with such procedures.

Definitions

2. In these Regulations –

"the Act" means the Insurance Act 1986;

"applicant" means a person or body seeking to effect a contract of insurance with an insurer (whether directly with an insurer or through an introducer) and includes a person specified in regulation 10;

"beneficial owner" means the individual who ultimately owns or controls the applicant or on whose behalf a transaction or activity is being concluded;

"board" means the board of directors of the insurer or, where the insurer has no board of directors, the governing body of the insurer;

"business relationship" has the meaning given by paragraph 2 of the Code;

[1] 1 986 c.24

Price £2.00

"the Code" means the Criminal Justice (Money Laundering) Code 2007[2];

"customer due diligence" means, in relation to an applicant or policyholder —

(a) carrying out the identification procedures specified in paragraphs 5 to 8 of the Code; and

(b) establishing the source of funds and source of wealth of that person in connection with the application or policy (as the context requires);

"enhanced customer due diligence" means the requirements as set out in these Regulations together with such additional reasonable measures appropriate to the degree of money laundering or terrorist financing risk associated with the proposed business relationship;

"FATF" means the Financial Action Task Force;

"Financial Crime Unit" means the Financial Crime Unit of the Isle of Man Constabulary;

"Guidance Notes" means the Guidance Notes made by the Authority under section 24C of the Act which apply to the class (or classes) of business undertaken by the insurer ;

"insurer" includes insurers which are authorised under section 6 of the Act or which hold permits issued under section 25 of the Act;

"introducer" means a person who by way of business, whether or not receiving commission, fees or other payment for the services provided, introduces an applicant to an insurer or undertakes the ongoing servicing of a policyholder;

"Money Laundering Reporting Officer" means an individual appointed by an insurer under paragraph 14(1) of the Code;

"politically exposed persons" means persons entrusted with prominent public functions, their immediate family members or persons known to have influence over the decisions of such persons;

"sanctions notices" means —

(a) lists of people and organisations designated and proscribed by the Isle of Man Government for the purposes of United Nations, European Union and national sanctions and other restrictive measures; and

(b) United Nations, European Union and national embargoes and restrictions on trading or other involvement with people, organisations or territories;

"senior management" means a director, chief executive or manager of the insurer.

Branches and subsidiaries

3. (1) Subject to paragraph (2), where an insurer has branches or subsidiaries in other jurisdictions, practices and procedures consistent with these Regulations must be operated throughout all parts of the organisation.

[2] SD 712/07

(2) An insu rer m ust meet the spe cific requ irements of regulato rs and author ities in those other jurisdictions. However, wher e the requirem ents of another jurisdiction differ from those required by these Regulations the insurer must comply with —

(a) the requirements of these Regulations; and

(b) any requirements imposed on the insurer in the other jurisdiction which are more onerous than those imposed by these Regulations.

(3) An insurer must inform the Authority when a foreign branch or subsidiary is unable to comply with paragraph (1) or (2). This notification is to be undertaken as soon as it becomes known to the insurer that a breach of this regulation has occurred.

Outsourced and delegated functions

4. Where an insurer outsources or delegates any functions (including where an insurer is m anaged by an insurance m anager or em ploys contractors) it rem ains the ultim ate responsibility of the insurer to ensure that th e activities or work carried out on its behalf are com pleted in accordan ce with these Regulations, and that adequate procedures are in place which meet the requirements of these Regulations.

Financing of terrorism

5. In addition to the prevention of money laundering, these Regulatio ns also apply to countering the financing of terr orism, and this m ust be cons idered by an insurer when establishing and carrying out procedures.

Non co-operative countries

6. (1) An insurer must have procedures in place to examine applicants who are situated or incorporated in any country appear ing on the list of FATF Non Co-operative Countries & Territories.

(2) W here an applican t is one to which paragraph (1) applies, the insurer m ust undertake appropriate enhanced custom er due diligen ce and m ust obtain sen ior management approval to continue the business relationship.

Waivers and concessions

7. (1) An insurer need not comply with regulations 8 to 14, 16, 24 and 25 where —

(a) a premium is payable to the insurer in one instalm ent of an amount not exceeding £7,500; or

(b) a regular prem ium is payable to the insurer and where the tota l payable in respect of any one calendar year does not exceed £2,500.

(2) An insurer need not com ply with regulations 8 to 14, 16, 24 and 25 where a policy has neither a surrender value nor a maturity value (for example, term insurance);

(3) Notwithstanding paragraphs (1) and (2), having paid due regard to the m oney laundering risk, an insurer may consider it appropriate —

(a) to comply immediately with the requirements of the regulations referred to in those paragraphs; or

(b) to comply with the requirements of the regulations referred to in those paragraphs, but to defer compliance until a claim is made or the policy is cancelled.

(4) Where a claim is made on a policy with neither a surrender value nor a maturity value (for example on the occurrence of an event), and the amount of the settlement is greater than that set out in paragraph (1)(a) or (b) (as the context requires) the insurer must undertake reasonable measures to satisfy itself as to the identity of the policyholder or claimant (if not the policyholder).

(5) Where a policy is cancelled resulting in the repayment of premium(s) and the amount of the settlement is greater than that set out in paragraphs (1)(a) or (b) (as the context requires), the insurer must undertake reasonable measures to satisfy itself as to the identity of the applicant or claimant (if different to the policyholder) and must also ensure it is satisfied as to the original source of wealth and source of funds.

(6) An insurer need not comply with paragraph (4) where settlement of the claim is to—

(a) a third party in payment for services provided (for example to a hospital where health treatment has been provided);

(b) a supplier for services or goods; or

(c) the policyholder(s) where invoices for services or goods have been provided to the insurer,

and the insurer believes the services or goods to have been supplied.

Customer due diligence

8. (1) Unless regulation 7(1) or (2) applies, where customer due diligence is required, it must be obtained as soon as is reasonably practicable after the applicant applies to enter into a business relationship with an insurer.

(2) In the event that an applicant is permitted to utilise a business relationship prior to the completion of the customer due diligence process, the insurer must apply risk management measures to control the type and volume of transactions that may be performed.

Customer due diligence requirements

9. (1) An insurer must undertake reasonable measures to verify the identity of the applicant and beneficial owner and satisfy itself as to the source of the applicant's funds and wealth. In the absence of satisfactory evidence the business relationship must not proceed any further.

(2) Where evidence of identity is required, an insurer must hold either original documents or suitably certified copies of original documents of identification on its

files, or must have undertaken a form of investigation which has satisfied the insurer as to the identification of the person concerned.

(3) An insurer must use reliable, independent source documents, data or information.

(4) An insurer must not delegate the responsibility for customer due diligence to another party. However, collection of information, including documents, may be delegated to an introducer in accordance with the requirements of regulation 21 or further outsourced in accordance with the requirements of regulation 22.

Beneficial ownership and controllers

10. (1**)** An applicant for a business relationship includes —

(a) the person(s) beneficially entitled to the assets to be used to fund a premium for the policy;

(b) any person who is able to exercise control over the policy; or

(c) any other person on whose behalf an applicant is acting.

(2) An insurer must undertake reasonable measures to establish the identity of a person, natural or legal, to which paragraph (1) applies in accordance with regulation 9.

Legal persons or bodies

11. (1) Where the applicant is a legal person or body, an insurer must satisfy itself as to the legal status of that person or body (including its existence and identity), its nature and that any person acting on its behalf is appropriately authorised to do so.

(2) An insurer must take reasonable measures to understand the ownership and control structure of the legal person or body.

Beneficiary of a life policy

12. The verification of the identity of a beneficiary named or nominated under a life insurance policy to receive any benefits arising following a claim or event may take place after the business relationship has been established provided that it takes place at or before the time of payout or at or before the time the beneficiary exercises a right vested under the policy. This regulation does not apply to a beneficiary under a trust.

Risk

13. (1) An insurer must assess the information required on each applicant or policyholder on a risk assessed basis in order to establish the inherent money laundering or terrorist financing risk.

(2) Where following such an assessment an applicant or policyholder is considered high risk, the insurer must undertake appropriate enhanced customer due diligence.

(3) An insurer must not apply simplified, or lower, levels of customer due diligence where there is a suspicion of money laundering or where the applicant or policyholder (including any party to the application or policy) is considered to be higher risk.

Purpose and intended nature

14. The insurer must satisfy itself (obtaining information where necessary) as to the purpose and intended nature of the business relationship.

Anonymous bonds etc

15. Anonymous bonds or contracts in fictitious names are not permitted and any such business relationships already in place must be treated as high risk and subjected to enhanced customer due diligence and ongoing monitoring.

Failure to obtain satisfactory evidence

16. Without prejudice to regulation 9(1), where an insurer is unable to obtain satisfactory evidence of identification it must consider making a suspicious transaction report to the Financial Crime Unit.

Complex and unusual large transactions etc

17. (1) An insurer must pay special attention to complex transactions, unusual large transactions, unusual patterns of transactions, and transactions that have no apparent or visible economic or lawful purpose, whether at inception or during the lifetime of a business relationship.

(2) An insurer must take reasonable steps to examine as far as possible the background and purpose of such transactions and to record its findings in writing. Whether the applicant is accepted by the insurer or not, the insurer must keep such records in accordance with regulations 28 to 30.

Existing business

18. (1) At any time during a business relationship the risk profile and circumstances of a policyholder or beneficial owner may change or additional information may come to the attention of an insurer. An insurer must continue to consider whether or not, at any time, additional customer due diligence information is required.

(2) The obligations of an insurer to consider and report any person are not limited to the application procedure nor is a transaction required to have occurred before additional information may be sought or a suspicion reported.

(3) An insurer must apply customer due diligence requirements to those parties referred to in regulation 10(1) on the basis of materiality and risk, and conduct due diligence on such existing relationships on a risk assessed basis in accordance with the requirements of regulation 13.

(4) Paragraphs (1) to (3) apply irrespective of any waiver under regulation 7(1) or (2) which applies, or has applied, during the business relationship.

Sanctions notices

19. (1) An insurer must have in place procedures which describe the system used to establish whether it maintains policies for the benefit of any of those individuals or organisations listed on, or transactions into jurisdictions appearing on, Sanctions Notices applicable to the Isle of Man.

(2) The procedures referred to in paragraph (1) must specify the actions to be taken should an individual, organisation or transaction be identified in respect of which a Sanctions Notice applies.

Politically exposed persons

20. (1) An insurer must have in place procedures to apply customer due diligence measures in respect of identifying whether any of the following is a politically exposed person —

(a) an applicant;

(b) a policyholder;

(c) a beneficial owner of an applicant or the person funding a premium paid under a policy;

(d) a settlor or trustee of a trust whose trustee is an applicant or policyholder;

(e) a beneficiary named or nominated under a policy;

(f) a beneficiary of a trust whose trustee is an applicant or policyholder; or

(g) any natural person having power to direct the activities of an applicant or policyholder.

(2) In the event that any person mentioned in paragraph (1) is identified as being a politically exposed person, an insurer must determine, on a risk assessed basis, whether or not to apply appropriate enhanced customer due diligence measures to the application for a business relationship.

(3) Simplified or reduced customer due diligence, as set out in the Guidance Notes, must not be applied to an application for a business relationship in the event that any person mentioned in paragraph (1) is identified as a politically exposed person.

(4) An insurer must obtain senior management approval to accept an application for a business relationship where any person mentioned in paragraph (1) is identified as a politically exposed person.

(5) Where an application for a business relationship has been accepted without the applicant, or any other person mentioned in paragraph (1), being identified as a politically exposed person, and such a person is subsequently found to have been or becomes a politically exposed person, the policy (or policies) must be referred to senior management.

(6) Where an insurer is in a business relationship with a politically exposed person, it must effectively monitor the relationship on an ongoing basis having due regard to the inherent money laundering risk.

(7) Failure to identify a person specified in regulation 20(1) as a politically exposed person will not automatically be considered a failure of systems or procedures

provided that reasonable and adequate measures have been undertaken in an attempt to make such an identification.

Introducers

21. (1) Where reliance is placed by an insurer in accordance with paragraph (3), before any business may be accepted from the introducer there must be in place written terms of business between the insurer and the introducer and the insurer must have in place written procedures in respect of the granting of such terms of business.

(2) An insurer must have procedures in place in respect of the ongoing monitoring of an introducer which must include information in respect of its regulatory status.

(3) Where an insurer is relying upon an introducer to collect information and evidence of identity or any form of customer due diligence on its behalf, and permits the introducer to retain this, it must take adequate steps to satisfy itself that copies of identification data and other relevant documentation relating to customer due diligence requirements will be made available to the insurer by the introducer upon request and without delay.

(4) In order to satisfy itself to the extent required under paragraph (3), an insurer must undertake random testing of its procedures to ensure that requested documentation is made available without delay.

(5) The ultimate responsibility for customer due diligence remains with the insurer, irrespective of the involvement of an introducer.

(6) Any written terms of business between the insurer and the introducer must include wording which requires the introducer to supply to the insurer upon request and without delay suitably certified evidence of the customer due diligence information in any particular case; and must require an introducer to maintain a record of the evidence for the required period (as specified in regulation 29).

Outsourcing

22. (1) Where there is a contract to outsource any functions concerning the administration or operation of an insurer in respect of customer due diligence the person undertaking the outsourced function is to be treated, for the purposes of these Regulations, as if it were the insurer and its customer due diligence processes and documentation will be considered to be those of the insurer itself.

(2) Paragraph (1) applies whether or not the outsourced function is undertaken by a member of the same group as the insurer.

Compliance monitoring and control

23. (1) An insurer must have adequate compliance management arrangements taking into account the size and risk profile of its business.

(2) The Money Laundering Reporting Officer, Compliance Officer(s) and other appropriate staff of the insurer must have timely access to customer identification data, other customer due diligence information, transaction records and any other relevant information sufficient for them to perform their respective roles.

Source of funds and source of wealth

24.(1) An insurer must make enquiries as to how an applicant has acquired the monies to be used as premium for, or contribution to, a policy.

(2) An insurer must establish how any payment is to be made, from where and by whom. Where payment is made from an account other than in the name of the applicant the reasons for this must be understood and recorded and where considered necessary evidence of identity of the account holder should be obtained.

(3) The insurer must be satisfied that the monies received have come from expected account(s).

Payment out of monies

25. Where payment of monies is to be made by an insurer to an account other than in the name of the policyholder the reasons for this must be understood, documented and the insurer must consider, on a risk assessed basis, whether evidence of identity of the account holder should be obtained.

Money laundering reporting officer

26. (1) A suitably senior person must be appointed by the board of the insurer as Money Laundering Reporting Officer. The Money Laundering Reporting Officer must be able to act independently and report on money laundering matters directly to the board of the insurer where necessary.

(2) In the case of an insurer authorised under section 6 of the Act, the person appointed for the purposes of paragraph (1) must be resident in the Isle of Man.

(3) A Money Laundering Reporting Officer shall be treated as a manager for the purposes of section 20 of the Act and the provisions of that section shall apply.

(4) Where an insurer has a branch or subsidiary in another jurisdiction, an officer resident in that jurisdiction may be appointed to deal with suspicion reports raised in that jurisdiction. However, the Money Laundering Reporting Officer retains overall responsibility for the role in all jurisdictions.

(5) Where an insurer appoints a Money Laundering Reporting Officer who is not an employee of the insurer (for example where a member of staff of the insurance manager of the insurer provides this service) the Money Laundering Reporting Officer must be of sufficient seniority and experience to undertake the role, and must have a right of direct access to the board of the insurer to be effective in the exercise of his or her functions.

(6) The Money Laundering Reporting Officer must have access to all documents and files, wherever held, as are required to undertake the role, whether or not within the scope of any agreement between the insurer and insurance manager.

(7) Where a Money Laundering Reporting Officer holds that position for more than one insurer, paragraphs (1) and (2) apply to each appointment.

(8) The Money Laundering Reporting Officer must submit, not less than annually, a report to the board of the insurer describing the business' anti-money laundering environment, progress on internal or external developments and activities undertaken during the reporting period and any money laundering or terrorist financing issues or risks to which the insurer may be exposed.

Suspicion reporting procedure

27. (1) An insurer must have procedures for raising suspicions by employees or directors and for subsequent reporting to the Financial Crime Unit.

(2) The obligation to make a report also applies to funds where there are reasonable grounds for the insurer to suspect that the funds are linked or related to, or to be used for terrorism, terrorist acts or by terrorist organisations or those who finance terrorism.

(3) All suspicious transactions, including attempted transactions, must be reported regardless of the amount or nature of the transaction.

Record keeping

28. (1) The records prepared and maintained by an insurer on its policyholder relationships and transactions must be such that —

(a) the requirements of all legislation, including the Code, these Regulations and the Guidance Notes, are met;

(b) competent third parties are able to assess the insurer's observance of money laundering policies and procedures;

(c) any transactions effected via the insurer can be reconstructed; and

(d) the insurer is able to satisfy, within a reasonable time, any enquiries or court orders from the appropriate authorities as to disclosure of information.

(2) Any records retained in electronic or microfilm format must be viewable and legible and be capable of being reproduced in a physical form at that is acceptable to the Authority and the courts of the Isle of Man and in accordance with the requirements of those courts.

(3) Reproduced records are acceptable if they are a true representation of the original physical document and must be legible, complete and sufficient to comply with the requirements of paragraph (1) or as otherwise specified by the Authority or the courts.

Retention periods

29. (1) For the purposes of regulation 21(6), the "required period" is at least 5 years from the date when —

(a) all activities relating to a one-off transaction or a series of linked transactions were completed;

(b) the business relationship was formally ended; or

(c) if the business relationship was not formally ended, when the last transaction was carried out.

(2) Where a report has been made to the Financial Crime Unit, or the insurer knows or believes that a matter is under investigation, the insurer must retain all relevant records for as long as required by the Financial Crime Unit.

Access to information

30. All customer due diligence records wherever held, and whether held by the insurer or not, must be available to the Money Laundering Reporting Officer, Compliance Officer and other competent staff for review and investigation purposes.

Staff screening

31. Every insurer and insurance manager must have in place appropriate and effective screening procedures when employing staff to ensure they have the integrity and abilities appropriate for their respective roles.

Training requirements

32. (1) An insurer must provide, or shall arrange provision of, appropriate and ongoing anti-money laundering and prevention of terrorist financing education and training for all staff. This must include —

(a) information on new developments;

(b) current money laundering and financing of terrorism techniques;

(c) methods and trends;

(d) a clear explanation of the relevant significant aspects of applicable laws and obligations; and

(e) the requirements concerning suspicious transaction reporting.

(2) The insurer must provide additional specific training appropriate for senior management, specific anti-money laundering staff and holders of relevant key control positions.

(3) Where an insurer outsources or delegates any functions, it remains the responsibility of the insurer to ensure that any staff who are undertaking any work on behalf of the insurer are trained in accordance with these Regulations.

Training records

33. Training records which demonstrate that appropriate training has been provided to all participants, including temporary staff, must be maintained by the insurer.

Training new employees

34. As soon as reasonably practicable after the commencement of employment, all new employees must be given education and training in the avoidance of money laundering and the prevention of terrorist financing in accordance with regulation 32.

Refresher training

35. (1) An insurer must provide, or arrange provision of, refresher courses at regular intervals, not less than annually, for senior management, specific anti-money laundering staff and holders of relevant key control positions, in order to maintain awareness and continued adherence to prevention procedures and regulatory requirements.

(2) Where there have been significant changes to legislative, regulatory or internal requirements or procedures, the insurer must provide, or arrange provision of, suitable training to make all staff aware of their responsibilities.

Compliance monitoring

36. An insurer must have procedures to ensure that the Money Laundering Reporting Officer, and Compliance Department if applicable, regularly monitors the implementation and operation of all anti-money laundering and terrorist financing procedures and controls. This must include monitoring the effectiveness of techniques employed for raising awareness and training of relevant staff.

Misuse of technological developments

37. An insurer must regularly consider, and where necessary have policies in place or take such measures as are needed, to prevent the misuse of technological developments for the purposes of money laundering or the financing of terrorism.

Offences

38. A person who contravenes a provision of these Regulations without lawful authority commits an offence.

Revocation

39. Paragraph 6 of Part II of Schedule 6 to the Insurance Regulations 1986 [3] (certification of compliance with requirements of the Common Trading Practices for Isle of Man Insurers) is revoked.

Made 20th June 2008

Chairman,
Insurance and Pensions Authority

---

[3] G.C. 319/86