



Anti-money laundering and counter-terrorist financing measures

British Overseas Territory of Gibraltar

Fifth Round Mutual Evaluation Report

December 2019



The Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism -

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

All rights reserved. Reproduction is authorised, provided the source is acknowledged, save where otherwise stated. For any use for commercial purposes, no part of this publication may be translated, reproduced or transmitted, in any form or by any means, electronic (CD-ROM, Internet, etc.) or mechanical, including photocopying, recording or any information storage or retrieval system without prior permission in writing from the MONEYVAL Secretariat, Directorate General of Human Rights and Rule of Law, Council of Europe (F-67075 Strasbourg or moneyval@coe.int)

The fifth-round mutual evaluation report on the British Overseas Territory of Gibraltar was adopted by the MONEYVAL Committee at its 59th Plenary Session (Strasbourg, 2-6 December 2019).

CONTENTS

EXECUTIVE SUMMARY	4
Key Findings	4
Risks and General Situation	7
Overall Level of Compliance and Effectiveness	7
Priority Actions	13
Effectiveness & Technical Compliance Ratings	15
MUTUAL EVALUATION REPORT	16
Preface	16
1. ML/TF RISKS AND CONTEXT	17
1.1. ML/TF Risks and Scoping of Higher Risk Issues	17
1.2. Materiality	21
1.3. Structural Elements	24
1.4. Background and Other Contextual Factors	24
2. NATIONAL AML/CFT POLICIES AND COORDINATION	33
2.1. Key Findings and Recommended Actions	33
2.2. Immediate Outcome 1 (Risk, Policy and Coordination)	35
3. LEGAL SYSTEM AND OPERATIONAL ISSUES	46
3.1. Key Findings and Recommended Actions	46
3.2. Immediate Outcome 6 (Financial Intelligence ML/TF)	49
3.3. Immediate Outcome 7 (ML investigation and prosecution)	62
3.4. Immediate Outcome 8 (Confiscation)	68
4. TERRORIST FINANCING AND FINANCING OF PROLIFERATION	78
4.1. Key Findings and Recommended Actions	78
4.2. Immediate Outcome 9 (TF investigation and prosecution)	81
4.3. Immediate Outcome 10 (TF preventive measures and financial sanctions)	89
4.4. Immediate Outcome 11 (PF financial sanctions)	95
5. PREVENTIVE MEASURES	99
5.1. Key Findings and Recommended Actions	99
5.2. Immediate Outcome 4 (Preventive Measures)	101
6. SUPERVISION	115
6.1. Immediate Outcome 3 (Supervision)	118
7. LEGAL PERSONS AND ARRANGEMENTS	134
7.1. Immediate Outcome 5 (Legal Persons and Arrangements)	136
8. INTERNATIONAL COOPERATION	144
8.1. Immediate Outcome 2 (International Cooperation)	145
TECHNICAL COMPLIANCE ANNEX	159
Recommendation 1 – Assessing risks and applying a risk-based approach	159
Recommendation 2 - National Cooperation and Coordination	163
Recommendation 3 - Money laundering offence	164
Recommendation 4 - Confiscation and provisional measures	167

Recommendation 5 - Terrorist financing offence	169
Recommendation 6 - Targeted financial sanctions related to terrorism and terrorist financing.....	172
Recommendation 7 – Targeted financial sanctions related to proliferation	178
Recommendation 8 – Non-profit organisations	181
Recommendation 9 – Financial institution secrecy laws.....	184
Recommendation 10 – Customer due diligence	186
Recommendation 11 – Record-keeping.....	191
Recommendation 12 – Politically exposed persons.....	192
Recommendation 13 – Correspondent banking.....	194
Recommendation 14 – Money or value transfer services	194
Recommendation 15 – New technologies	196
Recommendation 16 – Wire transfers.....	197
Recommendation 17 – Reliance on third parties.....	198
Recommendation 18 – Internal controls and foreign branches and subsidiaries.....	200
Recommendation 19 – Higher-risk countries.....	201
Recommendation 20 – Reporting of suspicious transaction.....	202
Recommendation 21 – Tipping-off and confidentiality.....	203
Recommendation 22 – DNFBPs: Customer due diligence	203
Recommendation 23 – DNFBPs: Other measures.....	205
Recommendation 24 – Transparency and beneficial ownership of legal persons.....	205
Recommendation 25 – Transparency and beneficial ownership of legal arrangements	210
Recommendation 26 – Regulation and supervision of financial institutions.....	212
Recommendation 27 – Powers of supervisors.....	215
Recommendation 28 – Regulation and supervision of DNFBPs	216
Recommendation 29 - Financial intelligence units	218
Recommendation 30 – Responsibilities of law enforcement and investigative authorities	221
Recommendation 31 - Powers of law enforcement and investigative authorities	222
Recommendation 32 – Cash Couriers	224
Recommendation 33 – Statistics	227
Recommendation 34 – Guidance and feedback	228
Recommendation 35 – Sanctions.....	229
Recommendation 36 – International instruments	230
Recommendation 37 - Mutual legal assistance.....	231
Recommendation 38 – Mutual legal assistance: freezing and confiscation	234
Recommendation 39 – Extradition	235
Recommendation 40 – Other forms of international cooperation.....	237
SUMMARY OF TECHNICAL COMPLIANCE – KEY DEFICIENCIES	243
GLOSSARY OF ACRONYMS.....	248

EXECUTIVE SUMMARY

1. This report provides a summary of the anti-money laundering and combating financing of terrorism (AML/CFT) measures in place in the British Overseas Territory of Gibraltar (hereinafter Gibraltar) as at the date of the on-site visit from 1 to 12 April 2019. It analyses the level of compliance with the FATF 40 Recommendations and the level of effectiveness of Gibraltar's AML/CFT system and provides recommendations on how the system could be strengthened.

Key Findings

- Gibraltar has a varied understanding of its money laundering (ML) and financing of terrorism (FT) risks. Whilst the key supervisors (the Gibraltar Financial Services Commission (GFSC) and the Gibraltar Gambling Commissioner (GGC)) have a robust understanding of risks at sectoral level underpinned by the collection of comprehensive data, the jurisdiction's understanding of the ML risk is affected by several shortcomings related to the NRA analysis, in particular by the limited analysis of quantitative and qualitative data and by underestimating the cross-border threat which Gibraltar faces as an international financial centre. The authorities demonstrated a good understanding of the risk of terrorism and FT typologies, whilst the assessment and understanding of the FT risk are affected by insufficient consideration of data available on transactions to/from conflict zones and high-risk jurisdictions. The risk related to cross-border transportation of cash is also insufficiently understood. Significant effort has been devoted by the authorities to raise awareness about the 2018 NRA findings, although the understanding of the results of the NRA and, in general, of the ML and FT risks by FIs and DNFBPs diverges. The authorities have acted upon the majority of the findings identified by the NRAs, implementing strategy and action plans, including following up on the findings of the most recent NRA. While several actions appear commensurate to some of the risks identified, the comprehensiveness of these strategies and action plans is affected by shortcomings concerning the assessment of risks. Cooperation and coordination with regard to both development and implementation of policies and at an operational level is one of the strengths of the overall AML/CFT system in Gibraltar. There are a number of exceptions to CDD requirements that are not predicated on an assessment of the risks.
- The Gibraltar Financial Intelligence Unit (GFIU) has increased its capacities in recent years and has extended cooperation with the LEAs and supervisory authorities, thus increasing its role in generating financial intelligence. However, the GFIU's analytical products were used by law enforcement agencies (LEAs) only to a limited extent and therefore did not have a significant impact upon developing investigations into ML and predicate offences. Better results were achieved with regard to FT investigations. LEAs did not prioritise cases concerned with the GFIU disseminations in their work. The suspicious transactions reports (STRs) which the GFIU receives are not of sufficient quality to assist them in performing their functions. The authorities have so far developed one strategic analysis which was not made available either to the oversight and supervisory agencies GFSC, GGC or to the private sector. Specific protective measures are in place to ensure the confidentiality of information exchanged, accessed or used.
- Since 2015 Gibraltar's AML/CFT legal framework has improved significantly and provides a solid basis for the authorities to detect, investigate and prosecute the ML/FT offence. Whilst this was followed by improvements in inter-agency cooperation and information exchange, the effective investigation and prosecution of ML offences remain undemonstrated. By the time of the on-site visit there have only been four ML convictions for self-laundering involving domestic predicates. There have been no successful third party and standalone prosecutions over the relevant period. Financial investigations are conducted regularly but these are often limited to providing further evidence in support of the prosecution of domestic predicate crime or pursuant to possible confiscation proceedings. Parallel financial investigations targeting ML are not pursued in cases where the associated predicate offences occur outside Gibraltar, thus

not reflecting the risks the jurisdiction has in its role as a financial centre. The judiciary applies the guidance of the sentencing guidelines council of England and Wales and the principles underpinning the sanctioning regime are well developed.

- Gibraltar's legislation provides all that is necessary for the detection, restraint and confiscation of the proceeds and forfeiture of the instrumentalities of crime, whether from domestic or international offending. It also provides non-conviction based civil recovery and cash seizure regimes as an alternative means of disrupting economic crime. Although confiscation is a policy objective, it has not been effectively pursued and the amount confiscated is low. There have been only two conviction-based confiscation orders, and these arose from crimes committed in Gibraltar. On the other hand, forfeitures of tobacco and instrumentalities used to smuggle (based on the 1997 Tobacco Act) were applied by Her Majesty's Customs (HMC) throughout the reporting period. Assets deriving from foreign predicates in complex and international cases remain undetected and therefore the benefit of that crime is neither restrained nor confiscated. Whilst LEAs have achieved results from cash seizures, the civil recovery regime has not yet been applied. The statistics on the confiscation of cross border movements of currency and bearer negotiable instruments (BNIs) suggest that this element in the overall confiscation regime has been underused.
- Gibraltar has recently updated its CFT legislation (predominantly the Terrorism Act 2018) and has equipped LEAs with tools and mechanisms to counter the financing of terrorism (FT). There has not yet been a T/FT prosecution in Gibraltar. Although the LEAs demonstrated an understanding of potential FT pathways that may occur in a financial centre, the relative lack of FT related STRs considered against the backdrop of transactions with conflict zones and high risk jurisdictions raises concerns as to whether the absence of FT prosecution is in line with the jurisdiction's risk profile. The LEAs have carried out several FT related investigations, all except one of which were triggered by STRs. FT investigations are given priority and the authorities observed that if there were to be a CT investigation it would always be accompanied by a parallel financial investigation. Gibraltar's investigation of suspected FT adopts and is integrated with the United Kingdom (UK) national CT strategy. It draws upon the close working relationship with the UK's law enforcement and security services and the experience, specialism, resources and expertise they provide in considering any FT related SARs, incoming FT mutual legal assistance (MLA) requests and activity in respect of high-risk jurisdictions. Any sentence imposed for FT in Gibraltar would follow the sentencing guidelines in England and Wales. The sentencing principles in FT cases in England and Wales are well developed and the sentences imposed in the UK are effective and proportionate. Some cases of FT investigations which did not result in prosecution due to what the authorities determined to be an insufficiency of evidence were pursued through disruptive procedures.
- Gibraltar currently has a comprehensive legal framework governing targeted financial sanctions (TFS) for FT and proliferation financing (PF). However, the new regime came into force only before the on-site visit, rectifying a number of identified deficiencies hampering the effectiveness of Gibraltar's TFS regime throughout the reporting period. Although the new legislation has introduced the legal gateway for many new mechanisms, standard operating procedures have not yet been introduced. Awareness of FT-related TFS in large financial institutions (FIs) is higher compared to the non-financial sector which has a less developed understanding of its obligations. In comparison to the FT-related TFS the awareness of PF related TFS within the private sector is low, particularly among DNFBPs. Most of FIs screen against all UN lists on automatic or semi-automatic checks for UNSCR updates, relying on commercial databases.
- No funds or other assets have been frozen in relation to designated persons or entities under the FT and PF-related TFS regime. Nevertheless, the GFIU has received STRs concerning potential matches with the UN-sanctions lists, which adds to the effectiveness of the FT-related TFS regime. The authorities have classified the vast majority of these STRs to be false –

positives.

- Reporting Entities' (REs) understanding of the ML risk is overall satisfactory albeit it varies across and within the sectors. Unlike ML risk, the FT risk is not properly understood by FIs (in particularly by banks, e-money providers, and MVTs). FIs focus almost exclusively on sanction screening, without proper consideration of transactions to high-risk countries, as evidenced by the low numbers of FT-related STRs. Some FIs (e.g. some banks) and TCSPs did not always demonstrate that they are taking measures that are commensurate to specific risk factors inherent to their businesses. The application of CDD measures varies across the FIs and DNFBPs. While TCSPs have a good understanding of the concept of beneficial owner (BO), this is not always the case for some other REs, including banks, particularly when complex ownership structures or trusts are involved. FIs and DNFBPs tend to overly focus on thresholds for identifying the BOs, which is an issue of concern particularly for the identification of targets for the implementation of TFS requirements. The quality of STRs can be questioned given the near absence of STR-triggered investigations, and their number is not commensurate to the risks that certain sectors are facing (particularly banks, e-money and TCSPs).
- All supervisory authorities apply licencing/registration and screening measures to prevent criminals and their associates from abusing FIs and DNFBPs. However, they target only new applications and not already licenced individuals. Although legal requirements do not extend to checking BOs and their source of funds, and there is no legal requirement to reject applicants with criminal background relevant for fit and proper, this is generally done in practice. The GFSC and the GGC have a robust understanding of risk. OFT is in its nascent stage, although it is developing fast. The other supervisors have an insufficient understanding of ML and TF risks. The GFSC primarily uses its Thematic Reviews for AML/CFT supervision which so far have been completed for the TCSPs and e-money sectors. On-site supervisory plans in the gambling sector are based primarily on the size of the entities concerned. Supervision for the rest of the FIs and DNFBPs is either triggered by events or is based on the general risk score that includes, but does not focus on, financial crime risk. In majority of cases sanctions are not proportionate and dissuasive. Communication between REs and supervisors is good whilst with regard to TFS, there is a need for better outreach to REs.
- Gibraltar has taken a number of measures to prevent the misuse of legal persons and arrangements for ML/FT purposes, including establishing the Register of Ultimate Beneficial Owners (RUBO). The risk of legal persons and arrangements' misuse for ML/FT purposes is understood only to some extent. Competent authorities can to obtain generally accurate and current basic information on all types of legal persons created in Gibraltar through the Companies House (CHG) and can obtain BO information directly from REs or rely on the RUBO. However, there are a number of factors that can affect the completeness and accuracy of the information as well as the timely access to such information.
- Gibraltar exchanges information and cooperate with its foreign counterparts (primarily from the UK and Spain) in relation to ML, associated predicate offences and FT. Competent authorities engage in all forms of international cooperation, including diagonal cooperation. An overall decrease in the number of outgoing requests for information has been observed in recent years whilst the timeliness of the information exchange is hindered by the shortage in human resources and the lack of clear guidelines in relation to incoming Mutual Legal Assistance (MLA) requests. The assistance provided by the GFIU has generally been commended by the global network. LEAs are active in the sphere of formal and informal cooperation using direct communication (police to police, customs cooperation), via liaison officers, Interpol, CARIN and other cooperation platforms. Competent authorities exchange basic and BO information on legal persons.

Risks and General Situation

1. The financial sector in Gibraltar accounts for approximately 20% of Gibraltar's GDP and consists primarily of branches or subsidiaries of international firms. The financial services provided by the Sector include banking, insurance, asset management, fund management as well as trust and company services. The Sector provides services primarily to non-resident clients, including clients from high-risk jurisdictions. Most of Gibraltar's banks offer and provide private banking to high-net worth individuals.
2. The NRAs conducted by Gibraltar identify organised crime as a threat due to the geographic proximity of the jurisdiction to areas where organised crime is active. According to the 2018 NRA over the last few years organised crime groups (OCGs) operating in the area of Spain's Campo de Gibraltar have increased their influence. Such OCG's are active in tobacco smuggling, particularly between Gibraltar and Spain and drugs trafficking, which create further high cash volumes. The main sources of criminal proceeds generated domestically are fraud, tobacco smuggling, tax crimes, drug trafficking and robbery/theft.
3. Electronic money (e-money) where the significant volumes of products and services offered in Gibraltar may facilitate speedy or anonymous transactions (including anonymous payments across borders), the Trust and Corporate Service Providers (TCSPs) sector, the MVTs and private banking (wealth management), have been identified in the 2018 NRA among the most vulnerable areas.
4. The authorities assess the FT risk as low to medium in Gibraltar. No cases of FT have been reached the prosecution phase so far, although several investigations have commenced during the period under review (2014-2018). According to the 2018 NRA there is no proof that this risk has materialised. The assessment team (AT) did not come across any evidence that there is a FT risk arising from links to OCGs operating in neighbouring countries.

Overall Level of Compliance and Effectiveness

5. Since the last evaluation, Gibraltar has taken steps to improve the AML/CFT framework. New legislation was introduced to strengthen the overall AML/CFT framework, which includes 2015 Proceeds of Crime Act, 2018 Terrorism Act, 2019 Sanctions Act, the 2014 European Freezing and Confiscation Orders Regulations (EFCO Reg.), and the 2017 European Investigation Orders Regulations (EIO Rags). The Proceeds of Crime Act has undergone significant changes and has been amended in part to transpose provisions of EU Directive 2015/849 and in part to further clarify and strengthen the national AML/CFT and confiscation of proceeds of crime regimes. Subsidiary legislation was also introduced to establish the ultimate beneficial ownership (UBO) registers for companies, trusts and foundations incorporated in Gibraltar. However, some deficiencies remain in Gibraltar's technical compliance framework.
6. The authorities' understanding of Gibraltar ML and FT risks is of varying degrees. They demonstrated a good understanding of the risk of terrorism and FT typologies, and a good understanding of some of the ML threats. However, the understanding of the ML risk is affected by several shortcomings related to the analysis of the cross-border threat that Gibraltar is facing as an international financial centre. In relation to tax crimes, Gibraltar authorities undertook a number of measures at policy level as shown by the number of agreements signed in the past years for the exchange of information for tax-enforcement purposes. On the other hand, the ML related risks that Gibraltar is facing concerning the laundering of these proceeds and the proceeds of other financial crimes committed abroad has not yet percolated at the GFIU and law enforcement level.

7. A moderate level of effectiveness has been achieved in identifying, understanding and assessing ML/FT risks, investigating and prosecuting FT, applying AML/CFT preventive measures by FIs and DNFBPs, implementation of FT-related TFS, on supervision of the financial and DNFBP sector, transparency of legal persons and arrangements and international cooperation. A low level of effectiveness has been achieved in all other areas covered by the FATF standards.

Assessment of risk, coordination and policy setting (Chapter 2; IO.1, R.1, 2, 33 & 34)

8. Gibraltar has made efforts to understand its ML/FT risks. The jurisdiction has a long-standing experience in ML risk assessment. Prior to 2016, when Gibraltar conducted its first NRA, a national threat assessment was conducted by the GFSC (2012 threat matrix) assessing the products and services which presented a ML risk to the jurisdiction. In September 2018, Gibraltar adapted the EUSNRA to Gibraltar's framework, assessing the products and services analysis of threats and vulnerabilities in the EUSNRA with the aims of both - contextualising it to Gibraltar and building on the findings of the 2016 NRA. This notwithstanding, the assessment of the ML/TF threat and of the ML/TF vulnerabilities was not always comprehensive.

9. Gibraltar has a varied understanding of its ML and FT risks. The authorities demonstrated a good understanding of the risk of terrorism, FT typologies and of some of the ML threats. The GFSC and the GGC have a robust understanding of risks at sectoral level, which is underpinned by the collection of comprehensive data. The jurisdiction's understanding of the ML risk is, however, affected by several shortcomings related to the NRA analysis, by the limited analysis of quantitative and qualitative data and in particular by underestimating the cross-border threat which Gibraltar faces as an international financial centre. The risk related to cross-border transportation of cash is also insufficiently understood.

10. The assessment and understanding of the FT risk are affected by insufficient consideration of data available on transactions to/from conflict zones and high-risk jurisdictions.

11. Significant effort has been devoted by the authorities to raise awareness about the 2018 NRA findings. Nonetheless, the understanding of the results of the NRA and, in general, of the ML and FT risks by FIs and DNFBPs varies.

12. The authorities have acted upon the majority of the findings identified by the NRAs, implementing strategy and action plans, including following up on the findings of the most recent NRA. While several actions appear commensurate to some of the risks identified, the comprehensiveness of these strategies and action plans is affected by shortcomings concerning the assessment of risks; the strategies and action plans were not revised and adapted to tackle new risks identified by the 2018 NRA.

13. Cooperation and coordination with regard to both development and implementation of policies and at an operational level is one of the strengths of the overall AML/CFT system in Gibraltar.

14. There are a number of exceptions to CDD requirements that are not predicated on an assessment of the risks.

Financial intelligence, ML investigations, prosecutions and confiscation (Chapter 3; IO.6, 7, 8; R.1, 3, 4, 29-32)

15. The GFIU has increased its capacities in recent years and has extended cooperation with the LEAs and supervisory authorities, thus increasing its role in generating financial intelligence. However, the GFIU's analytical products were used by LEAs only to a limited extent and therefore did not have a significant impact upon developing investigations into ML and predicate offences. This has partially been a consequence of the fact that LEAs did not prioritise cases concerned with

the GFIU disseminations in their work Better results were achieved with regard to FT investigations which all except one were triggered by STRs. There are also some concerns in relation to the quality of STRs which the GFIU receives. The authorities have so far developed one strategic analysis which was not, by the time of the on-site visit, made available either to the oversight and supervisory agencies (GFSC, GGC) or to the private sector.

16. There is no evidence to indicate that the GFIU's analysis and dissemination functions have ever come under any political, government or industry pressure. Specific protective measures are in place to ensure the confidentiality of information exchanged, accessed or used. This notwithstanding, further improvements in the GFIU's specialist software are required, particularly the analytical software program.

17. Since 2015 Gibraltar's AML/CFT legal framework has improved significantly and provides a solid basis for the authorities to detect, investigate and prosecute the ML/FT offence. Although this was followed by improvements in inter-agency cooperation and information exchange, the effective investigation and prosecution of ML offences remain undemonstrated. By the time of the on-site visit there have only been four ML convictions for self-laundering involving domestic predicates. There have been no successful third party and standalone prosecutions over the relevant period indicating that insufficient emphasis is placed by the LEAs on the detection, investigation and prosecution of cases potentially involving Gibraltar's FIs and intermediaries, targeting criminal property deriving from foreign predicates. Financial investigations are conducted regularly but these are often limited to providing further evidence in support of the prosecution of domestic predicate crime or pursuant to possible confiscation proceedings. Parallel financial investigations targeting ML are not pursued in cases where the associated predicate offences occur outside Gibraltar, thus not reflecting the risks the jurisdiction has in its role as a financial centre.

18. Gibraltar judiciary applies the guidance of the sentencing guidelines council of England and Wales and the principles underpinning the sanctioning regime are well developed. The judiciary also confirmed that they were entitled to depart from the guidelines and might, for example, impose higher sentences where the offending might have a tendency to undermine confidence in Gibraltar as a financial centre.

19. Gibraltar's legislation provides all that is necessary for the detection, restraint and confiscation of the proceeds and forfeiture of the instrumentalities of crime, whether from domestic or international offending. It also provides non-conviction based civil recovery and cash seizure regimes as an alternative means of disrupting economic crime. Although confiscation is a policy objective, it has not been effectively pursued and the amount confiscated is low. There have been only two conviction-based confiscation orders, and these arose from crimes committed in Gibraltar. On the other hand, forfeitures of tobacco and instrumentalities used to smuggle it (based on the 1997 Tobacco Act) were applied by HMC throughout the reporting period. Assets deriving from foreign predicates in complex and international cases remain undetected and therefore the benefit of that crime is neither restrained nor confiscated. Whilst LEAs have achieved results from cash seizures, the civil recovery regime has not yet been applied.

20. The statistics on the confiscation of cross border movements of currency and BNIs suggest that this element in the overall confiscation regime has been underused. The assessment team is of the opinion that a more in-depth analysis of the risks posed by the cross-border movement of cash is needed since the results of the seizure/confiscation of cash/BNIs transported across borders is only partially in line with the risks.

Terrorist and proliferation financing (Chapter 4; IO.9, 10, 11; R. 1, 4, 5–8, 30, 31 & 39.)

21. Gibraltar has recently updated its CFT legislation (predominantly the Terrorism Act 2018) and has equipped LEAs with tools and mechanisms to counter the financing of terrorism. There has not yet been a T/FT prosecution in Gibraltar. Although the LEAs demonstrated an understanding of potential FT pathways that may occur in a financial centre, the relative lack of FT related STRs considered against the backdrop of transactions with conflict zones and high risk jurisdictions raises concerns as to whether the absence of FT prosecution is in line with the jurisdiction's risk profile.

22. The LEAs have carried out several FT related investigations, all except one of which were triggered by STRs. FT investigations are given priority and the authorities observed that if there were to be a CT investigation it would always be accompanied by a parallel financial investigation. Gibraltar's investigation of suspected FT adopts and is integrated with the UK's national CT strategy. It draws upon the close working relationship with the UK's law enforcement and security services and the experience, specialism, resources and expertise they provide in considering any FT related SARs, incoming FT MLA requests and activity in respect of high-risk jurisdictions.

23. Any sentence imposed for FT in Gibraltar would follow the sentencing guidelines in England and Wales. The sentencing principles in FT cases in England and Wales are well developed and the sentences imposed in the UK are effective and proportionate. Some cases of FT investigations which did not result in prosecution due to what the authorities determined to be an insufficiency of evidence were pursued through disruptive procedures.

24. Gibraltar currently has a comprehensive legal framework governing TFS for FT and PF. However, the new regime came into force only before the on-site visit, rectifying a number of identified deficiencies hampering the effectiveness of Gibraltar's TFS regime throughout the reporting period. The relevant UN sanctions are now automatically applied in Gibraltar and the private sector is obliged to screen the UN designation lists. Awareness of FT-related TFS in large FIs is higher compared to the non-financial sector which has a less developed understanding of its obligations. Although the new legislation has introduced the legal gateway for many new mechanisms, standard operating procedures have not yet been introduced.

25. Gibraltar has identified the subset of NPOs falling under the FATF definition. The outcomes of the NPO specific NRA have been communicated to the sector. Most of the mitigating actions related to the risks faced by the NPO sector have been finalised. The NPO statutory bodies have a limited engagement with the GFIU, the GCID, LEAs and other state agencies, which does not allow them to appropriately assess new applicants and monitor activities. Some of the NPOs interviewed appeared to be unaware of the CFT measures in place and potential ways of NPOs' abuse for FT purposes.

26. No funds or other assets have been frozen in relation to designated persons or entities under the FT-related TFS regime. Nevertheless, the GFIU has received STRs concerning potential matches with the UN-sanctions lists, which adds to the effectiveness of the FT-related TFS regime. The authorities have classified the vast majority of these STRs to be false – positives.

27. The measures undertaken by the competent authorities of Gibraltar are consistent with the jurisdiction's overall FT risk profile. The relevant NPO statutory bodies did not reveal any indications of abuse of the NPO sector for FT purposes. There have been no NPO-related information requests by foreign competent authorities, or STRs filed. The authorities have not received a MLA request concerning FT matters within the review period. There have been no FT prosecutions or convictions.

28. Gibraltar has not frozen any assets or transactions as a result of PF-related TFS. In comparison to the FT-related TFS the awareness of PF related TFS within the private sector is low, particularly among DNFBPs. Most of FIs screen against all UN lists on automatic or semi-automatic checks for UNSCR updates, relying on commercial databases.

29. The authorities have indicated that the PF risk in Gibraltar is relatively low. This is also supported by the fact that Gibraltar is not a weapons or dual use goods producer and its port mainly serves as a transit point. HMC oversees the movement of dual use goods over the borders and provides and monitors export licenses. Among supervisory authorities, only the GFSC has taken some concrete actions in regard to the supervision of PF-related TFS.

Preventive measures (Chapter 5; IO.4; R.9–23)

30. Reporting Entities' (REs) understanding of the ML risk is overall satisfactory albeit it varies across and within the sectors. On the other hand, FT risks are not properly understood by FIs (in particularly by banks, e-money providers, and MVTS). FIs focus almost exclusively on sanction screening, without proper consideration of transactions to high risk countries.

31. FIs and DNFBPs that fall under the purview of the GFSC apply mitigating measures that are overall commensurate to their risks. However, risk assessment often is referred to as risk classification of the clients and not of all relevant risk factors. Some FIs (e.g. some banks) and TCSPs, did not always demonstrate that they are taking measures that are commensurate to these specific risk factors of their businesses.

32. Different degrees in applying CDD measures were exhibited by FIs and DNFBPs. While TCSPs have a good understanding of the concept of BO, this is not always the case for some other REs, including banks, particularly when complex ownership structures or trusts are involved. FIs and DNFBPs tend to overly focus on thresholds for identifying the BOs, which is an issue of concern particularly for the identification of targets for the implementation of TFS requirements.

33. FIs and TCSPs have a good understanding of the STRs legal requirements and of tipping off measures. However, there are certain concerns about the number of STRs filed by material sectors, their quality, and defensive reporting in the e-money and online gambling providers sectors. The understanding of TFS and their operational implications needs considerable improvement across all sectors, and particularly for smaller FIs and most types of DNFBPs. The understanding of TFS and their operational implications needs considerable improvement across all sectors, and particularly for smaller FIs and most types of DNFBPs.

Supervision (Chapter 6; IO.3; R.14, R.26–28, 34, 35)

34. All FIs established in Gibraltar, TCSPs, DLTs, auditors and insolvency practitioners, are licenced by the GFSC. Although legal requirements do not extend to checking BOs and their source of funds, and there is no legal requirement to reject applicants with criminal background relevant for fit and proper, this is generally done in practice. The screening measures consist in making inquiries to determine whether applicants have a criminal record, by way of obtaining criminal records and requiring applicant to declare through individual questionnaire any sanctions/convictions and investigations, both criminal and administrative imposed to them.

35. The GFSC and the GGC have a robust understanding of ML/FT risks. OFT is in its nascent stage, although it is developing fast. The other supervisors have an insufficient understanding of ML/FT risks. In case of accountants and tax advisors this shortcoming derives from the fact that they do not have a dedicated supervisor.

36. The GFSC uses primarily its Thematic Reviews for AML/CFT supervision. At the time of the onsite visit such reviews have been completed for the TCSPs and e-money sectors. Supervision for the rest of the FIs and DNFBPs that are licensed by the GFSC is either triggered by events or is based on the general risk score which, inter alia, includes financial crime risk. The number of inspections based on this approach, compared with those based on thematic reviews, is low. On-site supervisory plans in the gambling sector are informed primarily by the size of the entities concerned. Up until the end of 2018 the supervisory plans were also based on the number of SARs submitted.

37. In majority of cases sanctions imposed were not proportionate and dissuasive. Communication between REs and supervisors is good. This notwithstanding, there is a need for better outreach to REs.

Transparency and beneficial ownership (Chapter 7; IO.5; R.24, 25)

38. A number of measures to prevent the misuse of legal persons and arrangements for ML/FT purposes have been taken by Gibraltar (i.e. establishing the Register of Ultimate Beneficial Owners (RUBO), prohibiting bearer share warrants and subjecting TCSPs, which are used for setting up legal persons and arrangements, and subjecting TCSPs to licensing and to a comprehensive regulatory regime), however, important issues remain, which pose an inherent vulnerability to ML and FT of legal persons and arrangements that can be established in or managed from Gibraltar.

39. The 2018 NRA acknowledges the inherent risk to TCSPs in their creation and management of legal persons and arrangements, although the risk of their misuse for ML/FT purposes is understood only to some extent by Gibraltar.

40. Gibraltar has a robust system that allows relevant competent authorities to obtain through the CHG on timely manner and generally accurate and current basic information on all types of legal persons created in Gibraltar. However, legal ownership information that is registered refers primarily to TCSPs acting as nominee shareholders or directors.

41. BO information can be obtained by the authorities directly from REs (including TCSPs) or the RUBO in a timely manner. However, there are a number of factors that can affect the accuracy and adequacy of the BO information held by REs or in the RUBO (e.g. lack of an explicit record keeping requirement for BO information and the limited scope of information required to be filed in the RUBO concerning trusts, or to be kept by the companies).

42. Sanctions for non-compliance with the information filing requirements are available but limited (i.e. only in the case of late submissions and they are not proportionate or dissuasive).

International cooperation (Chapter 8; IO.2; R.36–40)

43. Gibraltar has a sound legal framework to exchange information and cooperate with its foreign counterparts in relation to ML, associated predicate offences and FT. Nevertheless, the timeliness of the information exchange is hindered by the shortage in human resources and the lack of clear guidelines in relation to incoming Mutual Legal Assistance (MLA) requests.

44. Legal assistance has been sought, primarily from the UK and Spain. However, the low number of outgoing requests in the period 2014-2018 raises concerns as to whether Gibraltar authorities proactively seek assistance. The indicated delays in receiving replies to requests for assistance and the limited resources that law enforcement agencies have at their disposal to pursue evidence abroad impede their capacity to investigate and disrupt transnational criminal networks involved in ML, drugs trafficking and tobacco smuggling. There have been no outgoing requests related to confiscation during the review period.

45. While extradition figures show that the vast majority of extradition requests is executed, in the case of non-EU countries, where the 1870 Extradition Act or the 2002 Fugitive Offenders Act (accessed via the TOCA) were applied, resulted into limitations on the extent of assistance Gibraltar could provide. Despite these complexities, Gibraltar recently executed such a request from Norway. The limitations in executing extradition requests from non-EU countries were recently mitigated with the introduction of the 2018 Extradition Act. Overall, deficiencies in the warrant can inevitably result in the non-execution of a request.

46. Competent authorities engage in all forms of international cooperation, including diagonal cooperation. An overall decrease in the number of outgoing requests for information has been observed in recent years. The GFIU rarely seeks information exchange for the purposes of its own analysis. The timeliness of its responses has generally been commended by the global network.

47. In terms of informal co-operation, the GFIU has a legal basis for the exchange of information with its foreign counterparts. This includes exchange of spontaneous information. Timeliness of its responses has improved since 2016. LEAs are also active in the sphere of informal cooperation using direct communication (police to police, customs cooperation), via liaison officers, Interpol, CARIN and other cooperation platforms. Supervisors reply to requests for information from foreign counterparts, although limited statistics were made available. The GGC exchanges information primarily with its UK counterpart. Competent authorities also exchange basic and BO information on legal persons with foreign counterparts.

Priority Actions

- Gibraltar should conduct a more comprehensive assessment of the ML external threats and vulnerabilities at national level. The assessment should particularly focus on i) the ML threat posed by proceeds generated by crimes committed abroad; and ii) inherent vulnerabilities which may be present at national (e.g. capacity/resource issues) and sectoral and products levels.
- Gibraltar should revise the FT risk assessment considering the GFSC's analysis of data concerning the geographic origin/destination of inflows and outflows of funds into/from the jurisdiction (both cash and wires) as well as a more robust and comprehensive analysis of the product-related FT vulnerabilities.
- Gibraltar should address the deficiencies identified in Technical Compliance Annex under R.26.
- Gibraltar should amend the POCA to extend the record keeping requirements to BOs and all CDD measures.
- Gibraltar should strengthen its STR regime by taking the following actions:
 - i. provide sector-specific training on indicators and typologies to increase the quality of STRs and to increase the level of reporting of ML and FT-related transactions, in a way that is commensurate to the threat that Gibraltar is facing.
 - ii. ensure, by way of outreach and enforcement during the inspections that gambling firms report only to the FIU and not also to the GGC, and that firms' internal procedures are aligned accordingly.
 - iii. increase awareness across all sectors on the legal framework applicable for the provision of additional information to the FIU.
- Gibraltar should assess the specific ML and FT risks related to legal persons and arrangements, including how the legal persons and legal arrangements may have been used to disguise

ownership or to launder the proceeds of crime and assess the specific inherent vulnerabilities to all types of legal persons that can be created in Gibraltar.

- The GFIU should carry out a review of the use of its analytical products by LEAs and based on this review streamline the intelligence gathering and subsequent reporting to LEAs with a view to improving the relevance of and impact of its products for triggering ML investigations.
- The GFIU's and LEAs' expertise as well as the already established inter-agency cooperation should be further developed to be able to focus more effectively on the sophisticated forms of ML in Gibraltar where predicates have been committed abroad.
- The LEAs should refine and apply a clear policy/strategy on ML investigations, setting out the range of circumstances in which a ML investigation should be commenced which reflects the risks of ML in Gibraltar, paying particular attention to the laundering of criminal property by elements within the financial sector and deriving from foreign predicates.
- The MLIU should treat each incoming MLA request in conjunction with the GFIU and with advice from the OCP&L as valuable intelligence that might be developed into a Gibraltar ML investigation, particularly into the possible ML by Gibraltar intermediaries and FIs.
- The LEAs and prosecutors should make better use of other criminal justice measures (such as civil recovery) where it is not possible to secure a ML conviction.
- LEAs should consistently carry out parallel financial investigations aimed at the detection of criminal property laundered in Gibraltar and that the results achieved are commensurate with the risk and context of Gibraltar.
- HMC should systematically apply its powers to detain falsely declared or undeclared cash or BNIs in order to determine whether there is a link with ML/FT or the associate predicate offences.
- The authorities (both LEAs and prosecuting authority) should formulate and/or further refine their policies and/or guidance documents on FT investigations and prosecutions, setting out the range of circumstances in which a FT investigation should be commenced and types of evidence likely to be required in a FT prosecution, reflecting the full range of FT risks likely to be encountered in Gibraltar.
- Sector specific FT guidance should be provided by the authorities to different FIs and DNFBPs to include risks /potential risks in transactions with conflict zones and other high-risk jurisdictions.
- The competent authorities should conduct further outreach to FIs and DNFBPs in relation to their compliance with obligations under the FT and the PF-related TFS regime and their applicability to BOs. In this context, further steps should be taken to ensure that designations and amendments to the FT and PF TFS regime are immediately communicated to all REs.
- Ensure that all supervisors adequately supervise and monitor PF-related TFS.

Effectiveness & Technical Compliance Ratings

Effectiveness Ratings¹

IO.1	IO.2	IO.3	IO.4	IO.5	IO.6	IO.7	IO.8	IO.9	IO.10	IO.11
ME	SE	ME	ME	ME	LE	LE	LE	ME	ME	ME

Technical Compliance Ratings²

R.1	R.2	R.3	R.4	R.5	R.6	R.7	R.8	R.9	R.10
PC	LC	C	LC	C	LC	LC	LC	C	LC
R.11	R.12	R.13	R.14	R.15	R.16	R.17	R.18	R.19	R.20
PC	PC	PC	LC	C	C	LC	LC	LC	C
R.21	R.22	R.23	R.24	R.25	R.26	R.27	R.28	R.29	R.30
C	PC	LC	PC	PC	PC	C	PC	C	C
R.31	R.32	R.33	R.34	R.35	R.36	R.37	R.38	R.39	R.40
LC	LC	C	C	LC	PC	C	C	C	LC

¹ Effectiveness ratings can be either a High- HE, Substantial- SE, Moderate- ME, or Low – LE, level of effectiveness.

² Technical compliance ratings can be either a C – compliant, LC – largely compliant, PC – partially compliant or NC – noncompliant.

MUTUAL EVALUATION REPORT

Preface

1. This report summarises the AML/CFT measures in place as at the date of the on-site visit. It analyses the level of compliance with the FATF 40 Recommendations and the level of effectiveness of the AML/CFT system and recommends how the system could be strengthened.
2. This evaluation was based on the 2012 FATF Recommendations and was prepared using the 2013 Methodology. The evaluation was based on information provided by the jurisdiction, and information obtained by the evaluation team during its on-site visit to the jurisdiction from 1 to 12 April 2019.
3. The evaluation was conducted by an assessment team consisting of:

Assessors

- Ms Alexandra Voinea, Financial Analyst, Financial Supervisory Authority of Romania (financial expert)
- Mr Giuseppe Lombardo, International Strategic Advisor, Financial Integrity (financial expert)
- Mr Mark Benson, Senior Prosecuting Advocate (Economic Crime), Attorney General's Chamber, Isle of Man (legal expert)
- Mr Artan Shiqerukaj, Vice General Director and Head of Operational and Investigation Department, General Directorate of Customs, Albania (law enforcement expert)
- Mr Michal Szermer, Chief Specialist in International Cooperation, Financial Intelligence Unit, Poland (law enforcement expert)

MONEYVAL Secretariat:

- Mr Lado Lalicic, Head of Unit
- Ms Veronika Mets, Administrator
- Mr Panagiotis Psyllos, Programme Assistant

4. The report was reviewed by Mr Matis Maeker, Head of the AML/CFT and PSP Supervision Department, Financial Supervision and Resolution Authority, Estonia, Mr Sorin Tanase Deputy Director, Directorate for Crime Prevention, Ministry of Justice, Romania, and the FATF Secretariat.
5. The British Overseas Territory of Gibraltar (hereinafter Gibraltar) previously underwent an IMF Assessment in 2007, conducted according to the 2004 FATF Methodology. The 2007 evaluation has been published and is available at <https://rm.coe.int/gibraltar-detailed-assessment-report-on-anti-money-laundering-and-comb/1680716081>.
6. Gibraltar's 2007 IMF Assessment concluded that the jurisdiction was compliant with 13 Recommendations; largely compliant with 19 Recommendations; partially compliant with 16 Recommendations; and non-compliant with 1 Recommendation. Gibraltar was rated compliant or largely compliant with 10 of the 16 Core and Key Recommendations.

1. ML/FT RISKS AND CONTEXT

7. Located at the southern tip of the Iberian Peninsula, Gibraltar has a land area of 6.8 square kilometres. It shares borders to the north with Spain and sea borders to the south with Morocco.

8. Gibraltar is a British overseas territory with over 33,000 resident population. In 2018 Gibraltar's GDP was approximately GBP 2.2 billion (2018)³. Gibraltar is a European territory for whose external relations a Member State, namely the United Kingdom, is responsible⁴. The local currency is the British pound sterling (GBP) and locally issued notes and coins of the same value in pounds and pence.

9. The current constitution (2006) provides for a degree of self-government which is compatible with British sovereignty of Gibraltar and with the fact that the UK is responsible for Gibraltar's external relations. In particular, the powers of the Governor are defined and the elected Government (Her Majesty's Government of Gibraltar) enjoys the remainder. The Governor's powers are limited to external relations, defence, internal security including certain aspects of policing and certain aspects of public services appointments. Notably, the UK retains international responsibility for Gibraltar, and as such is the Member State responsible for Gibraltar in the EU.

10. The Gibraltar Parliament is the legislative branch composed by 17 elected parliamentarians and a speaker. Representatives serve four-year terms. The head of government is the Chief Minister, who is the leader of the majority party with ten seats in parliament. A Council of Ministers appointed from the elected members of the parliament forms the Cabinet. The head of state is Queen Elizabeth II who is represented by a Governor appointed by Her Majesty.

11. As a separate jurisdiction to the UK, Gibraltar's government and parliament are responsible for the statute law, case law as decided by the courts, and the transposition of EU directives and the implementation of EU regulations into local law. However, Gibraltar's membership is not distinct from the UK's.

12. The judicial system of Gibraltar is based entirely on the English system, with minor modifications. There is a Magistrates' Court presided over by a Stipendiary Magistrate or by a Bench of lay Magistrates. The Supreme Court of Gibraltar has criminal, civil and family jurisdiction equivalent to that of the English High Court. As regards appeals, the Court of Appeal for Gibraltar is not resident and holds two sessions each year. The Justices of Appeal are, in the main, drawn from the English Court of Appeal.

13. Gibraltar ranks in the 80/102 in the 2019 Global Financial Centres Index. Its economy is primarily based on tourism, financial services, online gambling and shipping. Trade is concentrated on refined petroleum, passenger and cargo ships, cars, and recreational boats. The UK, Spain, Mauritania, Italy and the Netherlands are Gibraltar's main trading partners⁵.

1.1. ML/FT Risks and Scoping of Higher Risk Issues

1.1.1. Overview of ML/FT Risks

ML Threats

14. Gibraltar is an international financial centre (IFC) which faces various money laundering (ML) and financing of terrorism (FT) threats related to financial crimes, particularly with regard to the risk of laundering of proceeds of tax crimes committed abroad. Gibraltar's financial services

³ <https://www.gibraltar.gov.gi/new/sites/default/files/chief-ministers-budget-address.pdf>

⁴ Although it is part of the EU, Gibraltar is outside the customs union, the Common Agricultural Policy and the requirement to levy Value added tax. Moreover, Gibraltar does not form part of the Schengen Area. See <https://www.gibraltar.gov.gi/>

⁵ <http://data.imf.org/?sk=b7372cbe-e0dc-41a6-93ae-148b1676b69e>

industry provides services primarily to non-resident clients, including clients from high-risk jurisdictions.⁶ Most of Gibraltar's banks offer and provide private banking to high-net worth individuals. Figures from the Financial Services Commission's (GFSC) Financial Crime Return Data Analysis (30 June 2017) suggest that activities such as funds/money transfers, securities and TCSPs are popular among clients assessed as medium high⁷ and high risk⁸.

15. The NRAs conducted by Gibraltar identify organised crime as a threat due to the geographic proximity of the jurisdiction to areas where organised crime is active. According to the 2018 NRA over the last few years organised crime groups (OCGs) operating in the area of Spain's Campo de Gibraltar have increased their influence. Such OCG's are active in tobacco smuggling, particularly between Gibraltar and Spain and drugs trafficking, which create further high cash volumes.⁹ The main sources of criminal proceeds generated domestically are fraud, tobacco smuggling, tax crimes, drug trafficking and robbery/theft. HM Customs (HMC) figures for the period 2014 – 2019, show that tobacco and instrumentalities to a value of GBP 741,518.00 were forfeited under the 1997 Tobacco Act. Also, over the same period, assets worth of GBP 201,000 from drugs trafficking were frozen and seized.

16. The 2018 NRA identified the following main ML/FT risks (decreasing order): E-money; Conversion of funds; Creation of legal entities and legal arrangements; Retail financial sector-Deposits on accounts; Virtual currencies; Transfers of funds; Cash intensive business; Investment real estate; Payment services; Private banking-Deposits on accounts; Proximity to Organised Crime; Legal service from notaries and other independent legal professionals; Circumvent of international sanctions.

FT threats

17. The 2016 FT NRA assesses the FT risk as low to medium. No cases of FT have been reached the prosecution phase so far, although several investigations have commenced (see IO.9 par. 278-279) in Gibraltar during the period under review (2014-2018). The FT risk has been assessed for Gibraltar's products and services applying the EU Supra-National Risk Assessment findings. According to the 2018 NRA there is no proof that this risk has materialised. The AT did not come across any evidence that there is a FT risk arising from links to OCGs operating in neighbouring

⁶ According to the 2018 FSC Financial Crime Data Analysis, the client base of the financial sector consists of 27% residents and 73% non-resident (individuals and corporates) clients. This number does not include the e-money sector where the vast majority are non-resident clients.

⁷ According to the Analysis in 2016 approximately 573.000 clients were residents of medium high-risk jurisdictions and 424 clients were residents of high-risk jurisdictions. According to the report the list of countries which are considered of high risk includes countries listed by the FATF as high risk jurisdictions and countries which score equal or greater than 7.00 in the 2016 BASEL AML Index report - <https://www.baselgovernance.org/asset-recovery/basel-aml-index>. Also, the list of countries which are considered of medium high includes countries holding a score between 6.00 and 7.01 in the 2016 BASEL AML Index report.

⁸ According to the 2018 FSC Financial crime analysis of firms' data, the total number of non-resident high-risk customer relationships in 2018 amounted in 6829 individual customers and 255 corporate and trust customers, corresponding in 0.28% of the share of all customer relationships in Gibraltar or 2.9% excluding the e-money customers. Note the same individual customers may appear several times in these figures because individuals and businesses will often have multiple financial relationships.

⁹ A 2014 report of OLAF recommended to launch judicial investigations both in Spain and in Gibraltar on organised crime. OLAF expressed a number of concerns "regarding the link between a significant increase in the size of the Gibraltar market for cigarettes over the past four years and the subsequent increase of cigarette smuggling across the frontier and corresponding increase in size of the illicit market in southern Spain". See <https://www.telegraph.co.uk/news/worldnews/europe/gibraltar/11026733/Money-laundering-and-smuggling-over-Gibraltar-border-on-the-rise-says-EU.html>

countries. The 2018 NRA acknowledges that the e-money and the MVTS sectors present the highest risk of being used by perpetrators and terrorist groups to finance their activities.

Vulnerabilities

18. The 2018 NRA identifies, two risk areas with the highest ML/FT vulnerability score (4)¹⁰: a) electronic money (e-money)¹¹ where the significant volumes of products and services offered in Gibraltar may facilitate speedy or anonymous transactions (including anonymous payments across borders) and a significant volume of higher risk customers; and b) virtual currencies which can be connected with prepaid credit cards¹² allowing access to fiat currency.

19. A significant ML vulnerability score (3) is attributed in the 2018 NRA to the risk of funds conversion, to the Trust and Corporate Service Providers (TCSPs) sector, to private banking (wealth management), to the proximity of OCGs (organised criminal groups), to the securities and funds sector and to tobacco sales¹³. Unauthorised currency-exchange may also be exploited for criminal activities.

20. Other overarching vulnerabilities within the national system include the ineffective seizure and confiscation of criminal proceeds resulting from predicate offences and the lack of investigations and prosecutions of standalone ML cases. A lack of experience in conducting financial investigations, particularly in the Customs Department (HMC), has been identified by the authorities as an issue of concern. The high-turnover of staff in the G-FIU and the lack of capacity and resources in LEAs (see analysis of IO6, IO7 and IO8) also have an impact on Gibraltar's vulnerability to ML. The lack of experience of HMC and other LEA officers may have contributed, in part, to a vulnerability in the effective identification and securing of assets.

1.1.2. Country's Risk Assessment & Scoping of Higher Risk Issues

Country's risk assessment

21. Gibraltar conducted its first NRA in April 2016¹⁴ (2016 NRA), using an in-house-developed methodology¹⁵. This assessment relied more on qualitative data gained from both private and public sector¹⁶ than quantitative data. The 2016 NRA presents "risk events", assessed in terms of

¹⁰ According to the 2018 NRA ML/FT risk are assessed based on the following scoring scale: 1 = Lowly Significant; 2 = Moderately Significant; 3 = Significant; 4 = Very Significant.

¹¹ Pre-paid debit and or credit cards are a form of e-money in Gibraltar.

¹² Note that since the transposition of the 4th AMLD in May 2015 the limit to anonymous electronic money is restricted to EUR 250.

¹³ <https://www.eubusiness.com/news-eu/gibraltar-britain.xdm>

¹⁴ In 2012, a threat Matrix for Gibraltar's financial sector was produced by the FSC (2012 threat matrix) assessing the products and services which presented a ML threat to the jurisdiction. The threat matrix included impact and likelihood assessments, and threat descriptions. Based on the qualitative data and input of the private sector. Reporting entities (REs) were required to factor in this threat matrix into their own risk-based approach (RBA). The threat assessment was subject to updates in order to reflect evolving and new threats in the regulated financial sector.

¹⁵ The public version of the NRA was formally published in April 2016 although the non-public version was available to public sector stakeholders as from November 2015.

¹⁶ Relevant competent authorities (the Attorney General's Chambers, EUID/LSU Finance Centre Director, the FSC, the Gambling Commissioner; Gibraltar Coordinating Centre for Criminal Intelligence and Drugs (GCID); Gibraltar Financial Intelligence Unit (GFIU); Gibraltar Regulatory Authority; HMC and Royal Gibraltar Police (RGP) and private sector (e.g. Association of Trust and Company Managers, Gibraltar Association of Compliance Officers (GACO), Gibraltar Banker's Association, Gibraltar Betting and Gaming Association, Gibraltar Chamber of Commerce, Gibraltar Federation of Small Businesses and Gibraltar Society of Accountants) contributed in developing of the 2016 NRA. Contrary to them, lawyers and real estate agents (REAs) were not engaged in the process, due to the absence of an appointed AML/CFT regulator for these sectors at the time.

impact and likelihood. Some important sectors and products were not assessed by the 2016 NRA. The fact that the banking sector and its products were not assessed was a significant shortcoming, given the materiality and risk posed by this sector. The 2016 NRA was complemented by a separate FT risk assessment in general and by a FT risk assessment of the NPO sector in particular. An Action Plan was drafted based on the 2016 NRA findings. In this Action Plan each of the identified NRA Risks was assigned to a lead public authority responsible for the design and delivery of a mitigation programme. Specific actions were determined, including milestones and delivery dates agreed with the National Co-Ordinator for AML/CFT (NCO). As a result of the 2016 NRA, the FT NRA and the NPO FT Risk Assessment, the Cabinet of HM Government of Gibraltar (HMGoG) produced the 2017 Strategic Response paper in support of the objectives set by each public sector authority.

22. Following the publication of the EU Supra National Risk Assessment (EUSNRA), Gibraltar conducted its second NRA in 2018¹⁷. The NCO undertook the revision of the 2016 NRA in an effort to apply the threats and risks (including new risks) set out in the EUSNRA to those found in Gibraltar.

23. In reviewing the Gibraltar national risk assessments, AT considered the rigour of the process and procedures employed; and the internal consistency of the assessment, including whether the conclusions are reasonable given the information and analysis used. As noted under the analysis of IO1, the AT has reservations on the risk classification of the 2018 NRA (for example, online gambling providers are not included among the highest risk sectors, despite the materiality and risk posed by this sector (see IO6 and IO9). Generally, the quality of the analysis, (based primarily on products and services) lacks a holistic approach in understanding and assessing the overall risk that a particular sector, or the jurisdiction as a whole, may face, applying the findings of the EUSRA to the context encountered by Gibraltar.

Scoping of Higher Risk Issues

24. In this context, assessors are of the view that the major ML risks in Gibraltar currently relate to the following areas:

25. **Trust and Company Service Providers (TCSPs)** – As at the time of the on-site visit, there were 2535 trusts in Gibraltar established and administered by 58 licensed professional trustees registered with the GFSC Register for Regulated Entities.¹⁸ The 2018 NRA attributes a significant ML-related vulnerability score to the sector, whilst according to the 2017 GFSC Analysis TCSPs' activities are attractive to medium and high risk clients. The focus of the assessment team was on how well ML/FT risks are mitigated by TCSPs and, in particular upon the identification of the beneficial owners (BOs) of TCSP clients.

26. The ML threat of **on-line gambling** was rated as significant by the NRA. The total gross gaming yield (deposits- withdrawals) for Gibraltar operators in 2018 was GBP 6.5 billion. The sector has approximately 10 million active customers at any given time.¹⁹ The AT considered how well ML/FT risks were mitigated in this sector including the application of customer due diligence (CDD) measures.

27. **Non-resident clients** – Gibraltar is an IFC with a non-resident client base. According to the 2018 GFSC Financial Crime Return Data Analysis 1.81% of clients of Gibraltar's financial sector

¹⁷ The 2018 NRA was distributed on the 14th of September 2018 by publication on the GFIU's and each of the Supervisory Bodies' web-sites.

¹⁸ According to figures provided by the authorities, there are also 20,670 TCSP accounts and customers, 1/5 of which refers to non-resident customers. <http://www.gpsc.gi/regulated-entities/professional-trustees-13>

¹⁹ Note that, there is a lot of double counting, as a customer usually has a relationship with two or more operators which has not been taken into account.

reside in medium-high risk jurisdictions²⁰ and 0.28% in high risk jurisdictions. The assessors sought to explore the understanding of the private sector of ML/FT risk deriving from non-resident clients, the appropriateness of client risk segmentation and the focus on the mitigating measures in place.

28. **ML investigation, prosecution and conviction** – the AT sought to determine whether what was identified as a relative lack of experience in the area of financial investigations had evolved over the course of the review period. The assessment team also sought to explore the extent to which ML activities were investigated and prosecuted and the level of cooperation among LEAs and FIs in relation to the initiation of ML investigations which might lead to autonomous prosecutions, especially in cases where predicate offences were committed abroad.

29. The use of **E-money** has been identified in the NRA as one of the risk areas with the highest ML/FT vulnerability score and the highest ML/FT risk in Gibraltar. There are four e-money/card issuers²¹ currently operating from Gibraltar. The e-money sector has the largest client base in Gibraltar with 2,291,113 (2,290,547 non-resident and 566 resident) individual and 39,238 (of which only one resident) corporate clients. The total e-money outstanding issued money (including IDT Financial Services limited) was GBP 225,526,315 (2018). The AT considered the extent to which the sector has been abused by perpetrators, the industry's understanding of these risks and the adequacy of the mitigating measures in place.

30. The AT sought to explore the following factors: whether the **Transfer of Funds** through MVTs and banking has been employed by perpetrators in order to evade international sanctions; the measures implemented by the financial sector, particularly MVTs, to identify the source of funds (cash or e-money) specifically when those funds were transferred to high risk jurisdictions; and to explore the sanctions-related level of awareness of the MVTs sector.

31. **Border controls** – bordering Spain and near the north coast of Africa, Gibraltar is exposed to the trafficking and smuggling of goods. Despite strict controls at entry points, illicit cross border tobacco trading itself may generate large volumes of illicit cash. The AT considered the effectiveness of controls at the borders to detect false/non-declarations and identify ML/FT suspicions. The control systems at the port (including cargo controls) were also discussed with the responsible authorities.

32. **Private banking (wealth management)** – the ML threat and vulnerability of private banking is significant. Given the low level of suspicious transaction reports (STRs) and the high ML risk exposure of the sector,²² the assessment team explored the reasons behind the low number of STRs and the adequacy of the legal framework and controls in place for high risk customers and high-risk jurisdictions.

33. **Virtual currencies** – Gibraltar has regulated firms operating through the use of DLT and therefore virtual currencies. The evaluation team considered the measures taken by the authorities to understand and decrease the ML/FT risk in this area, including market entry controls and supervision. The assessors also focused on the issue of proper identification and controls applied by financial technology entities (Fintech).

1.2. Materiality

34. Gibraltar is an IFC. Gibraltar's economy is dominated by four sectors – tourism; shipping and port services; financial services; and on-line gaming. Gibraltar is included in the Global

²⁰ Medium High – Countries holding a score between 6.00 and 7.01 in the 2018 BASEL AML Index report.

²¹ At the time of the on-site a fifth e-money issuer was in the process of surrendering its authorisation.

²² NRA pg.15

Financial Centres Index which ranks the competitiveness of financial centres and is widely quoted as a source for ranking such centres. At March 2019, Gibraltar was placed in 80th place (out of 102 centres).

35. The financial sector accounts for approximately 20% of Gibraltar's GDP and consists primarily of branches or subsidiaries of international firms. The financial services provided by the Sector include banking, insurance, asset management, fund management as well as trust and company services. There are 11 authorised credit institutions with total banking deposits GBP 5.9 billion, 76,193 active customers²³ and GBP 10.4 billion funds under management (April 2019). Insurance companies and e-money institutions are the most actively used types of financial services (see tables 2 and 3).

36. Detailed information on the materiality of the financial sector is available in the following tables.

Table 1: incoming and outgoing transactions in 2018

Sector	Incoming transactions (GBP)	Outgoing transactions (GBP)
Banks	64,223,583,948	68,324,422,312
E-Money	3,313,472,626	2,482,808,507
Fund administrators	2,292,867	1,596,843
Funds	97,165,029	88,809,678
Insurance companies (life)	106,837,131	64,967,080
Insurance intermediaries (life)	53,861,872	550,000
Investment firms	428,079,635	191,639,234
Pension advisors	4,401,785	4,067,884
Total	68,232,078,983	71,159,200,710

Table 2: Summary of Activity in FATF High Risk Jurisdictions

		2017	2018
No. of transactions	Received	922	1,548
	Issued	1,647	3,758
Value of funds	Received	GBP 25,236,605	GBP 6,581,961
	Issued	GBP 4,369,194	GBP 25,068,365
Average value per transaction	Received	GBP 23,372	GBP 4,252
	Issued	GBP 2,653	GBP 6,670

Table 3: Active number of customers in 2019

Sectors	Individuals	Corporate and Trusts
Banks	69,673	6,520
Bureau de Change	27,065	585
Electronic Money	2,291,113	39,238
Fund Administrators	35	102
Fund Managers	28	14
Funds	279	324
Insurance Companies(Life)	92,968	1,237
Insurance Intermediaries(Life)	5,825	97
Investment Firms	2394	1,508

²³ Approximately 97% of the banking sector customers resides in low and medium-low risk countries. The risk classification is based on the 2018 BASEL AML Index report.

Pension Advisors	14	4
Pension Controllers	4625	234
Trust & Company Service Providers	15877	11,450
Total	2,509,986	61,313

Table 4: Insurance sector in 2019

Sector	Number of entities/agents	Total assets, minus liabilities (GBP)	Gross written premium (GBP)
Life Insurance	4	609,270	73,667
Life Insurance Intermediaries	18		
Insurance Managers	7		

Table 5: Other sub-sectors in 2018

Sector	Number of entities/agents	Total assets, minus liabilities (GBP)
E-Money Institutions	4	432 mil.
MVTS	14	4.4 mil.
Investment Services	27	127.1 mil.
Funds	62	1,450 mil.

37. Turning to the Fintech sector, since 2017 there has been a drive by HMGoG to create a favourable regulatory environment for Fintech companies, by regulating the use of distributed ledger technology (DLT). The sector is supervised by the GFSC.

Table 6: Fintech products and services present in Gibraltar

Product/Service	Licensed	Regulated	Supervised	No. of active entities
DLT Providers - licensed to use DLT for storing or transmitting value belonging to others in connection with the operation of a secondary market and out of these	Yes	Yes	GFSC	8
DLT Provider - Acting as a broker/dealer <i>(In addition to the operation of a secondary market)</i>	Yes	Yes	GFSC	2
DLT Provider - provision of custody services <i>(In addition to the operation of a secondary market)</i>	Yes	Yes	GFSC	4
DLT Provider - provision of wallet services <i>(In addition to the operation of a secondary market)</i>	Yes	Yes	GFSC	1
Initial coin offerings (ICOs), Token offerings and Utility Token ICOs	Yes (only securities tokens)	Yes (only securities tokens) Utility Token ICOs are subject to AML/CFT requirements only	GFSC	Approx. 60 active ICOs in 2018

38. All forms of DNFBPs listed by FATF are active in Gibraltar (see table 4). The most important sectors are on-line gaming sector, accounts for approximately 25% of Gibraltar's GDP.²⁴ In 2016, approximately 30% of the global online gaming sector, estimated at GBP 30 billion, was generated in Gibraltar.²⁵ According to the authorities there are 35 licensed remote operators.

39. TCSPs also play an important role in Gibraltar's non-financial sector (approximately GBP 31 million net worth of assets were managed by the sector in 2018). Overall, the TCSPs business is internationally oriented, focusing mainly on the UK market.

40. Other types of DNFBPs appear to consist of smaller numbers of professionals. The real estate sector structure ranges from construction companies to real estate agencies. For high value dealer (HVDs), this ranges from vehicles to antiques' shops. Lawyers and legal firms are the largest groups among independent legal professionals. More information on the DNFBP sector is available under the DNFBP section below.

1.3. Structural Elements

41. The key structural elements needed for an effective AML/CFT regime are present in Gibraltar. It is a politically and institutionally stable jurisdiction, based on accountability, transparency and the rule of law. Responsibility for developing and implementing AML/CFT policy in Gibraltar is shared between the relevant authorities, the roles of which are well defined.

42. Since 2015 Gibraltar has implemented several reforms in its AML/CFT system triggered by its NRA processes and the application of the 4th EU AML Directive.

43. The 2019 agreement²⁶ between the UK and Spain to combat tax fraud and ML in Gibraltar once the UK leaves the EU adds to the stability of the jurisdiction.

1.4. Background and Other Contextual Factors

1.4.1. AML/CFT strategy

44. Gibraltar has acted upon most of the findings identified in its NRAs, implementing strategy with action plans. It has followed up on the findings of the most recent NRA. The 2017 AML/CFT strategy outlines the high-level strategic outcomes (prevention, detection, enforcement, international cooperation and awareness-raising), with specific actions for attaining them. Most of the measures envisaged by the action plans and strategy were implemented by the authorities, with some exceptions (see immediate outcome 1). The strategy is informed by the risks identified by the 2016 NRA, as well as by the FT risks identified by the FT and NPO risk assessments. There are no immediate plans to revise the strategy in light of the revised 2018 NRA, as the authorities consider that the 2017 action points remain pertinent. The continued relevance of the 2017 AML/CFT strategy is to some extent questionable (see IO.1).

45. Each strategic outcome has been assigned to a leading agency responsible for reporting upon and delivering the required actions or working with others where the actions are shared between agencies. The NCO has reviewed the specific action plans that each stakeholder authority has designed (which are endorsed by HMGoG) to mitigate the specific risks identified in the NRA.

46. Driven by the Strategy and results of the 2018 NRA, the GFSC conducted specific thematic AML/CFT reviews on the e-money and TCSP sectors and increased data collection efforts to inform

²⁴ <http://www.independent.com.mt/articles/2017-05-12/local-news/Brexit-Malta-set-to-benefit-if-gaming-companies-leave-Gibraltar-6736174168>

²⁵ <https://www.ednh.news/brexit-could-threaten-gibraltars-online-gaming-sector/>

²⁶ <https://www.dw.com/en/spain-and-uk-sign-gibraltar-tax-deal-ahead-of-brexit/a-47770067>

their assessment of the firm, sectoral and jurisdictional risks which have been shared with the NCO.

1.4.2. Legal & institutional framework

47. The AML/CFT legal and organisational framework in Gibraltar is governed by the Proceeds of Crime Act (POCA), the 2011 Crimes Act, the 2018 Terrorism Act, and the 2019 Sanctions Act as well as other Acts and Regulations.

48. The main agencies in Gibraltar's institutional structure involved in implement AML/CFT regime are as follows:

49. **The Cabinet of HM Government of Gibraltar** holds ultimate responsibility for the implementation of policies, legislation and resourcing of the Government Departments and Agencies involved in the application of mitigation measures and the identification of AML/CFT risks.

50. **The Minister for Commerce and the Minister for Justice** are responsible for meeting FATF standards which form part of the portfolio of the Minister for Commerce which includes Financial Services and Gambling operators. The Minister for Justice's portfolio includes, as expected, the Judiciary and Prosecutions as well as legal drafting responsibilities.

51. **The National Co-ordinator for AML/CFT (NCO)** was established in June 2017 in order to co-ordinate the national AML/CFT framework. The Attorney General of Gibraltar was appointed to this role on the same day as the legislation came into force. The role includes undertaking and updating NRAs; providing advice on policy and operational matters designed to mitigate identified ML/FT risks; and delivery of the strategic and operational action plans by stakeholder authorities.

52. **The Gibraltar Financial Intelligence Unit (GFIU)** is the central authority for the receipt, analysis and dissemination of information related to ML/FT. The GFIU's functions, powers and responsibilities are regulated in accordance with the POCA.

53. **The Royal Gibraltar Police (RGP)** was formed in 1830 and is the second oldest British police force in the world, second only to the Metropolitan Police in London. The RGP is responsible for policing economic crime and working in partnership with other stakeholders such as the Gibraltar Financial Services Commission and the GFIU. To this end, the RGP operates an Economic Crime Unit (ECU) subdivided into two disciplines, the Money Laundering Investigation Unit (MLIU) and the Fraud Squad. The MLIU's primary responsibility is to enforce Gibraltar's Anti Money laundering (AML) and the Countering the Financing of Terrorism (CFT) regimes. It is also required to discharge its responsibilities towards the Annual Policing Plan set by the Gibraltar Police Authority. The MLIU investigates all ML offences relating to all types of profit generating predicate offences as well as pursuing ML offences on a stand-alone basis. The MLIU is responsible for asset recovery. POCA powers provide for a post-conviction confiscation regime and non-conviction based civil recovery.

54. **Her Majesty's Customs (HMC)** are the customs and import authority of Gibraltar. It is a uniformed, enforcement body, under the responsibility of the Ministry of Finance. The HMC is responsible for carrying out customs duties, checking both commercial goods and individuals entering with possessions into Gibraltar. It is also empowered to carry out financial investigations.

55. **The Gibraltar Coordinating Centre for Criminal Intelligence and Drugs (GCID)** is a multi-agency intelligence unit which coordinates and provides to LEAs all source intelligence against drug traffickers and organised crime. The GCID is subject to direction and policy from HE the Governor and the Chief Minister jointly. It acts in support of the Gibraltar LEAs and does not undertake operational duties. Since 2002, the GCID performs the function of Interpol Gibraltar.

56. **The Gibraltar Financial Services Commission (GFSC)** is the regulator of providers of Gibraltar's financial services whether conducted in Gibraltar or other jurisdictions, such as the UK. In particular, the GFSC regulates and supervises credit institutions, e-money and payment institutions, bureau de change, TCSPs, investments and consumer credit firms, funds, insurance companies and managers, insurance intermediaries, insolvency practitioners, pension trustees and controllers, regulated market participants and auditors. The GFSC is governed by the 2007 Financial Services Commission Act.

57. **The Gambling Commissioner (GGC)** is responsible for the regulation of the gaming sector. The Gambling Act provides for two separate entities to oversee the licensing and regulation of the gambling industry in Gibraltar, namely; the Licensing Authority and the GGC. The former carries out its statutory responsibilities with the assistance of the Gambling Division (GD) of the Ministry of Commerce.

58. **The Office of Fair Trading (OFT)** is responsible supervisory authority for regulating high value dealers (HVD) and real estate agents. It was established in 2016 and it is governed by POCA.

59. **The Registrar of the Supreme Court (RSC)** has the operational lead for the registration and supervision of the legal profession, with a Legal Profession Supervision Officer responsible for AML / CFT issues (POCA Schedule 2). The Chief Justice is ultimately responsible for regulating the admission of barristers and solicitors to practice in the Supreme Court, their professional practice, conduct and discipline.

60. **The Board of Charity Commissioners (BCC)** is a regulatory body governed by the Charities Act. The Board is appointed by the Minister with responsibility for Finance and the tenure is generally a period of two years. The Board holds plenary meetings periodically about four times a year. All charities in Gibraltar are registered with the BCC.

61. **The Office of Parliamentary Counsel (OPC)** is a part of the Government Law Offices (GLO). Its work is divided into three distinct areas: domestic, European Union, and international. The OPC is responsible for identifying the most appropriate legislative solutions for the issues in hand, for liaising with Ministers and department officials to ensure that EU obligations are properly satisfied and for reviewing the requirements of new international treaties and submitting jurisdiction reports on existing treaties.

AML/CFT/CPF Co-operation and co-ordination mechanisms

62. Cooperation and coordination among stakeholders take place through the office of the NCO and the Interagency Working Group, where all main stakeholders are represented, all policy and operational matters are co-ordinated and discussed to give effect to the desired outcomes. Additionally, ad-hoc meetings take place between the NCO and stakeholder authorities as well as between the authorities themselves outside of formal groupings to ensure co-operation. Formal gateways exist in the NCOR and POCA as well as the FS(IG&C) A which permit a free exchange of relevant information between all stakeholder authorities and competent authorities.

1.4.3. Financial sector and DNFBPs

Financial sector

63. Gibraltar's financial sector is composed of banks, e-money providers (EMIs), funds and fund administrators, payment Service providers (PSPs), bureaux de change, DLT providers, investment firms, consumer credit and mortgage providers, life and general insurance companies and intermediaries.

64. The banking sector is the largest in terms of assets and is considered a high-risk sector by the GFSC. There are 11 authorised credit institutions with total banking deposits of GBP 5.9 billion

and with GBP 10.4 billion funds under management (31 December 2018)²⁷. Over the review period, a total of 5 banks have closed their offices in Gibraltar, and a foreign branch is in the process of being sold. Currently, the GFSC is examining 3 new applications for banking license: a government owned bank established to cover the gap in retail financial services; a privately-owned institution and an online bank targeting high income clients from Western Europe, including Chinese expatriates.

65. Over the last five years the banking sector has witnessed a series of transformation and a shift from more traditional banking to modern, Fintech banking.

66. As of January 2019, the following non-bank FIs were subject to supervision by the GFSC:

Table 7: Number of Non-bank Financial Institutions supervised by the GFSC

Type of Entity	No. Licensed/Regulated/Supervised
Insurance Industry	35
Securities Industry	29
Electronic Money Institutions	4
Payment Institutions	1
Pension Advisors	9
Pension Controllers	21
Currency Exchange Operators	11
Fund Managers	46
Fund Depositories	4
Fund Administrators	8
Funds	51

67. As of January 2019, the following DNFBPs were subject to AML/CFT supervision:

Table 8: Number of supervised DNFBPs by supervisory authority

Type of Entity	No. Licensed/Regulated/Supervised	Licensing and AML/CFT supervisory authority
Real estate agents	45	OFT
HVD	2 (which are registered as DPMS)	OFT
High risk dealers (HRDs) ²⁸	31	OFT
Lawyers and legal firms	250	RSC
Notaries	12	RSC
Accountants	14	FS
Auditors	14	GFSC
Insolvency practitioners	22	GFSC
TCSP	59	GFSC
Casinos (land-based)	2	GGC
Remote B2C gambling	16	GGC
Remote B2B gaming	17	GGC
Betting shops	1	GGC
Non-Casino Gaming Machine Suppliers	8	GGC
Non-Casino Gaming Machine Premises	124	GGC

²⁷ The total number of banks acting at the time of the on-site in Gibraltar is 11 compared to 15 as of the end of 2017. During this period 4 banks surrendered their licence for purely investment reasons.

²⁸ HRDs are dealers in goods which have not received a payment above the monetary threshold (GBP 8,000); and are considered by the OFT to have a higher inherent risk and vulnerability to ML/FT.

68. The gambling sector comprises of business to business (B2B) and business to customer (B2C) operators. The sector has changed significantly between 2014 and 2018 since the number of B2C operators dropped from 22 to 16 and the number of B2B operators doubled from 8 to 17.

69. The DNFBPs sector also includes 45 real estate agents (REAs) registered in Gibraltar, 4 HVDs that receive cash payments above the threshold of GBP 8.000, of which 2 are dealers in precious metals and stones (DPMS).

Materiality and level of ML/TF risks of the different FIs and DNFBPs

70. The types of services and products offered in Gibraltar by FIs (particularly banks, fund administrators and managers) and DNFBPs (particularly TCSPs, lawyers, real estate agents and HVDs to a lesser extent) cater primarily to non-resident customers (high-net-worth individuals (HNWI)) for, inter alia, asset management and protection, and for privacy, and the minimisation of tax burdens. As a result, most financial services have an international nature and present an inherently higher ML and (albeit to a lesser degree) FT risk. The GFSC figures show that out of 10,294 clients introduced in 2017 (0,88% of all new customers on-boarded in 2017), 7,684 (0,65% of all new customers on-boarded in 2017) were introduced by eligible introducers.²⁹ Gibraltar-licensed TCSPs are involved in the creation and management of complex ownership structures through the provision of several services, including acting as a trustees, nominee shareholder and providing directorship and other company and trust-related services. Fund administrators and managers manage the wealth of non-resident customers and HNWIs. Lawyers also assist those businesses that wish to carry out a regulated/licensed activity from Gibraltar (e.g. online casinos and e-money providers). The online gambling operators' industry and e-money providers sector are particularly developed in Gibraltar.

71. The assessors classified the obliged sectors based on their importance within the Gibraltar context, given their respective materiality and level of ML/FT risk. This classification was applied to inform the AT's conclusions throughout the report (particularly in IO.3 and IO.4), with a greater weighting being given (whether positively or negatively) according to the relative importance of the sector to the AML/CFT framework.

1.4.4. Preventive measures

72. The cornerstone of the AML/CFT preventive measures in Gibraltar is POCA³⁰ which came into force in 2015 to give full effect to the 4th EU AMLD. The Act lists the supervisory authorities responsible for AML/CFT and introduced new supervisors for sectors that were not covered by the previous legal framework. Alongside the POCA, the Supervisory Bodies Powers Regulations (SBPR) came into force in 2017 and gives supervisors the necessary powers to enforce the POCA requirements.

73. There are instances where the scope of the POCA is wider or narrower than the FATF Recommendations, partly on a risk-sensitive basis. It extends to the broad range of gambling services, as the CDD requirements apply to all gambling services. The POCA also applies to DLT providers. POCA, however, has a number of exceptions which are not based on risk (see analysis of R1 in the TCA).

74. Aside from the POCA, the legal framework is complemented by Guidelines issued by each respective regulator or supervisor.

75. The Guidelines issued are as follows:

²⁹ FSC Financial Crime Return Data Analysis.

³⁰ Its predecessor was adopted in 1990.

76. FIs and TCSPs, insolvency practitioners and auditors should comply with the Guidelines issued by the GFSC (AMLGN). Those are constantly updated, with the latest version in force since February 2019.

77. Gambling providers are guided by 2 sectoral Codes of Practice, the General Gambling Guidelines (2016) and the Remote Gambling Guidelines (2018). The General Gambling Guidelines consider natural persons as land-based casino customers (B2C), while the Remote Gambling Guidelines apply to B2C and B2B activities.

78. HDVs and REAs have 2 separate, but similar Guidelines that must be considered. The latest update is dated February 2019. One of the most important changes is the stipulation in the introduction that the notes should be regarded as regulatory standards for the purposes of the POCA and are enforceable pursuant to POCA and the Supervisory Bodies (Powers etc.) Regulations 2017. Prior to February 2019 the notes stated that any information contained was not intended to be legal advice and was for guidance and information purposes only.

79. Lawyers, notaries and other legal professionals have in place Guidance notes issued by the RSC with the aim of assisting lawyers and notaries in Gibraltar in meeting their obligations under the Gibraltar AML/CTF regime.

80. No sectoral guidance has been issued for Accountants and Tax Advisors.

1.4.5. Legal persons and arrangements

81. The main law governing the creation and regulation of legal persons in Gibraltar is the Companies Act (CompA). Further information can be found under R.24-25. All companies created in Gibraltar are subject to mandatory registration with the Companies House Registry (CHG). All different types, forms and basic features of legal persons, public and private companies limited and unlimited companies are described in the CompA, sectoral laws and online on the CHG website.

82. The following table presents the types of legal persons available in Gibraltar and provides a description of their functions.

Table 9: Overview of legal persons in Gibraltar

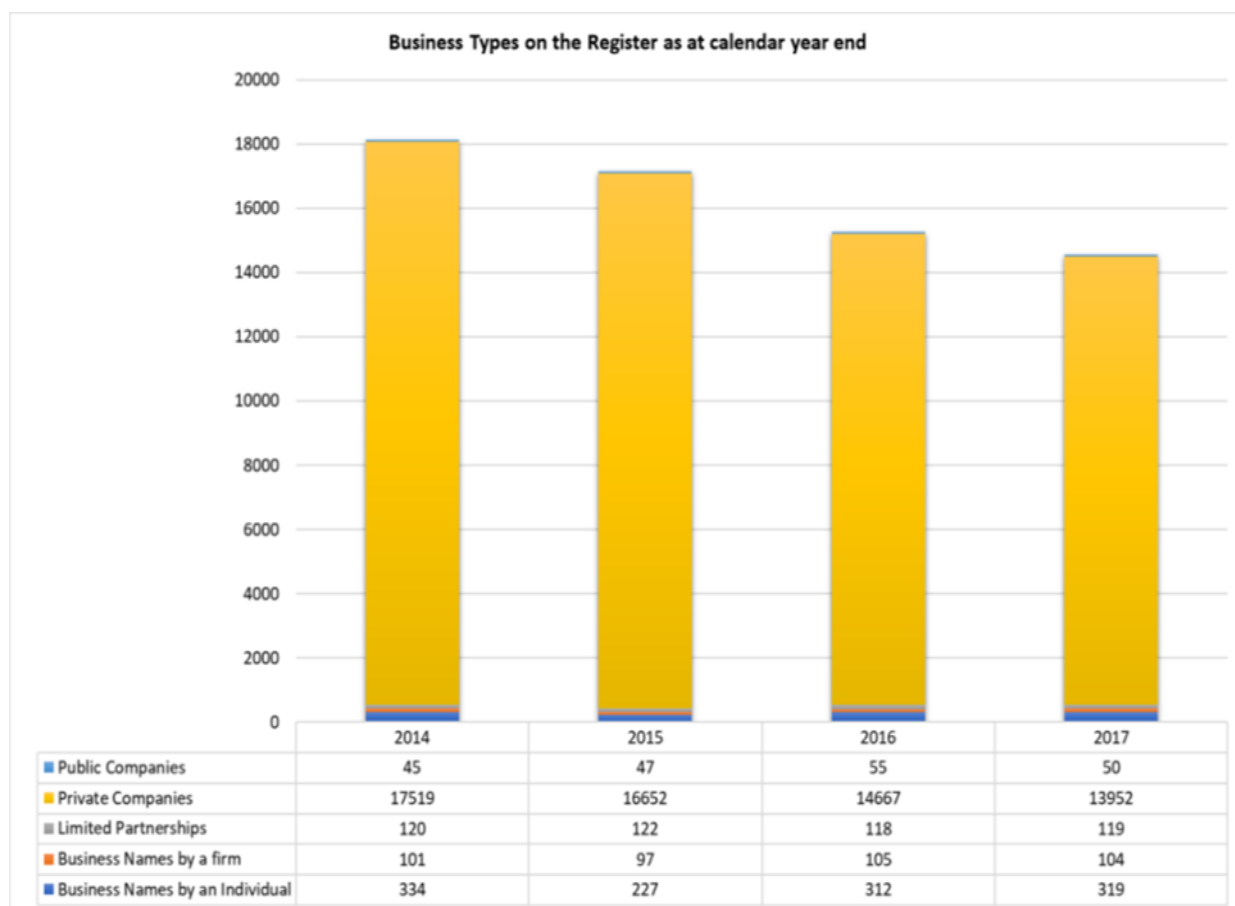
DESCRIPTION	NUMBER	Description
Private Company	16147	A Private company is one which, by its articles of association: 1. Restricts the right to transfer shares; 2. Prohibits any invitation to the public to subscribe for its shares or debentures
Public Company	48	A public company, i.e. a company whose articles do not contain the above restrictions, must have at least seven shareholders, and two directors, and, if formed as such, is not allowed to commence business until it has obtained a trading certificate from the Registrar of Companies
Private Company limited by guarantee with or without share capital	363	Most Companies Limited by Guarantee are used for various purposes usually not for profit organisations, including clubs, charities, community activities and property management so as to obtain corporate status. They would come under the category of Private or Public Companies depending on their size.
Public Company limited by guarantee with or without share capital	0	Separate legal personality with members who act as guarantors. Profits may be distributed to its members. Used primarily for incorporating multi-stakeholder organisations
Foreign Company carrying	133	Branches of foreign companies

on business in Gibraltar		
European Company (Societas Europaea)	0	The European Company Statute (Council Regulation (EC) No 2157/2001 (the "Regulation") created a new form of company – the European Company or Societas Europaea. This type of company is available to commercial bodies with operations in more than one Member State. Its use will be entirely voluntary. It may be created on registration in any Member State of the European Economic Area. An SE that has been formed and registered in one Member State may subsequently transfer its registration to any other Member State
Limited Liability Partnership	14	Same characteristics as a normal partnership in terms of tax liability but provides reduced financial liability to each partner. Used primarily for professions which normally operate as a traditional partnership, such as solicitors and accountancy firms.
European Economic Interest Grouping	4	An EEIG is a type of legal entity created under the European Community (EC) Council Regulation No. 2137/85. It is designed to facilitate or develop the economic activities of its members by a pooling of its resources, activities or skills. An EEIG is not a EU company but a vehicle allowing companies or individuals of different Member States to combine and register in any EU country a grouping that has legal personality and can operate across national frontiers. It is formed to carry out particular tasks for its member owners and is quite separate from its owners' businesses. It is not intended that the grouping would make profits for itself, however. Any profits would be apportioned among the members and taxed accordingly, and in this it is similar to a partnership. The EEIG is not subject to corporate tax. It has unlimited liability.

83. There are six types of companies in Gibraltar: private company; public company; foreign company carrying on business in Gibraltar; a re-domiciled foreign company; company limited by guarantee with or without a share capital; and a European company.

84. There are four European Economic Interest Groupings registered in Gibraltar.

Table 10: Business Types on the Register



1.4.6. Supervisory arrangements

85. The GFSC is responsible for the authorisation, regulation and supervision of all FIs. The GFSC, in performing its duties, operates under the POCA and the list of Supervisory Acts (GFSC(SA)O). The GFSC is also responsible for supervising some DNFBPs such as TCSPs, auditors and insolvency practitioners

86. The supervision of the gambling sector (casino and online gambling) is undertaken by the GGC, with the assistance of the Gambling Division (GD). The GGC performs its duties under POCA and the Gambling Act.

87. The OFT has been appointed supervisory authority under POCA for HVDs and REAs since 2016. Accountants and Tax Advisors are also required to obtain a business license from the OFT, but in the absence of a prescribed supervisory authority the default supervisor for AML/CFT is the Financial Secretary.

88. The RSC has the operational lead for registration and supervision of legal professions with the Chief Justice ultimately responsible for admission of barristers and solicitors to practice. The RSC is assisted by the Legal Profession Supervision Officer for AML/CFT supervision of the profession and who has administrative support from the staff of the Court Service.

1.4.7. International cooperation

89. Gibraltar has a sound legal framework to exchange information and cooperate with its foreign counterparts in relation to ML, associated predicate offences and FT. The central authority for receiving incoming MLA requests is the Attorney General (AG). Extradition requests are

received by the Governor, whose powers are delegated to the Chief Secretary. Both MLA and extradition requests are reviewed by the OAC. Requests relate to drugs trafficking, ML and computer fraud and corruption.

90. Competent authorities engage in all forms of international cooperation, including diagonal cooperation and LEAs have formal and informal cooperation using direct communication (police to police, customs cooperation), via liaison officers, Interpol, CARIN and other cooperation platforms. Legal assistance has been sought, primarily from the UK and Spain.

91. Supervisors reply to requests for information from foreign counterparts (the UK, the US, Spain and other EU member states), although limited statistics were made available.

92. Competent authorities exchange basic and BO information on legal persons.

93. The authorities of Gibraltar take active part in the work of multilateral fora both at policy and at the operational level, such as MONEYVAL, the Anti-Money Laundering Operational Network (AMON), Interpol, CARIN and the Egmont Group.

2. NATIONAL AML/CFT POLICIES AND COORDINATION

2.1. Key Findings and Recommended Actions

Key Findings

Immediate Outcome 1

- a) Gibraltar has a varied understanding of its ML and FT risks. The authorities demonstrated a good understanding of the risk of terrorism, TF typologies and of some of the ML threats. The GFSC and the GGC have a robust understanding of risks at sectoral level, which is underpinned by the collection of comprehensive data. The jurisdiction's understanding of the ML risk is, however, affected by several shortcomings related to the NRA analysis, by the limited analysis of quantitative and qualitative data and in particular by underestimating the cross-border threat which Gibraltar faces as an international financial centre.
- b) The assessment and understanding of the FT risk are affected by insufficient consideration of data available on transactions to/from conflict zones and high-risk jurisdictions. The risk related to cross-border transportation of cash is also insufficiently understood.
- c) Gibraltar demonstrated an understanding at policy level of the risk posed by tax crimes, as shown by the number of agreements signed in past years for the exchange of information for tax-enforcement purposes. However, the understanding of ML risks related to tax predicates, and the cross-border threat that Gibraltar faces concerning the laundering of both these proceeds and of financial crimes in general has not yet percolated down to the GFIU and law enforcement level.
- d) The assessment of vulnerabilities, both for ML and TF, was not always comprehensive and was often limited to considering whether a given product or service was subject to preventive measures and did not take into account resource/capacity issues that LEAs are facing.
- e) Significant effort has been devoted by the authorities to raise awareness about the 2018 NRA findings. Nonetheless, the understanding of the results of the NRA and, in general, of the ML and FT risks by FIs and DNFBPs varies. This may be due to an excessively top-down approach which did not fully involve all stakeholders in the analysis process and did not always result in a full buy-in to the findings of the NRA, particularly the 2018 NRA.
- f) The authorities have acted upon the majority of the findings identified by the NRAs, implementing strategy and action plans, including following up on the findings of the most recent NRA. While several actions appear commensurate to some of the risks identified, the comprehensiveness of these strategies and action plans is affected by shortcomings concerning the assessment of risks; the strategies and action plans were not revised and adapted to tackle new risks identified by the 2018 NRA and no comprehensive follow-up was undertaken in respect of the actions envisaged in the GFSC's analysis of transactions to/from conflict zones and high risk jurisdictions.
- g) Cooperation and coordination with regard to both development and implementation of policies and at an operational level is one of the strengths of the overall AML/CFT system in Gibraltar.
- h) There are a number of exceptions to CDD requirements that are not predicated on an assessment of the risks.

Recommended Actions

Immediate Outcome 1

The authorities should:

- a) Conduct a more comprehensive assessment of the ML external threats that Gibraltar is facing. The assessment should particularly focus on the threat posed by proceeds generated by crimes committed abroad or of a transnational character (such as smuggling of cigarettes and drug trafficking) particularly the ML risks of tax and financial crimes (e.g. corruption) committed in foreign countries, whose proceeds may be laundered in Gibraltar. Assess to what extent domestic OGCs could pose a threat to Gibraltar
- b) Conduct a more comprehensive assessment of the ML risk drawing conclusions from more statistics, particularly the data collected by the GFSC on financial crime and on transactions to/from high-risk countries. The types of statistics collected by the GFSC and GCC should, to the extent possible, be collected in a more systematic way for all sectors, including DNFBPs that fall under the purview of other supervisors and be used to identify, assess and understand more comprehensively the risks in those sectors.
- c) Conduct a more comprehensive assessment of the vulnerabilities, that is focused on both inherent vulnerabilities which may be present at national (e.g. capacity/resource issues) and sectoral and products levels, (e.g. the effective implementation of existing measures). Review the risk classification of the 2018 top risk factors, applying this more comprehensive approach to the assessment of threats and vulnerabilities.
- d) Assess the risk that may be posed by cash, particularly cross-border transportation of cash.
- e) Revise the FT risk assessment considering the GFSC's analysis of data concerning the geographic origin/destination of inflows and outflows of funds into/from the jurisdiction (both cash and wires) as well as a more robust and comprehensive analysis of the product-related TF vulnerabilities.
- f) Use the updated NRA or sector specific assessments to justify any exemption, enhanced or simplified measures and ensure that exemptions from any AML/CFT obligations or requirements for enhanced measures are based on the results of risk assessments.
- g) Update the 2017 strategy to take into account the increase in risks identified in certain areas by the 2018 NRAs (for example the proximity to organised crime) and the new risks identified, which were not identified in the 2016 NRA (e.g. the use of products in the banking sector, cash intensive businesses and international sanctions), as well as the findings of the GFSC's analysis of transactions concerning conflict zones/high risk jurisdictions. The action points attached to the Strategy should tackle more effectively the high turnover in staff in the GFIU.
- h) The GFSC should follow up on the actions identified in its 2017 analysis of transactions with conflict zones, particularly compliance by reporting entities (REs) with the TF-related STR obligation, with targeted inspections in those firms that appear to be under-reporting or that have rejected/exited business relationships on the basis of tampered CDD data provided by the customers. The background and rationale of transfers to/from high-risk jurisdictions should be investigated to the extent possible, particularly in those cases where the rationale of the transfers may not be evidently clear.
- i) The Interagency working group should consider establishing the Steering Committee envisaged by the 2017 Strategy. The Steering Committee should have a clear mandate on PF.
- j) Increase the efforts to promote a better understanding of risks across the REs, particularly the

FT and NPO risk, and focusing on DNFBPs, including through the engagement of industry associations.

94. The relevant Immediate Outcome considered and assessed in this chapter is IO.1. The Recommendations relevant for the assessment of effectiveness under this section are R.1, 2, 33 and 34.

2.2. Immediate Outcome 1 (Risk, Policy and Coordination)

2.2.1. Country's understanding of its ML/FT risks

95. Gibraltar has a varied understanding of its ML and FT risks. Although the authorities demonstrated a good understanding of the risk of terrorism, of FT typologies and of some of the ML threats that Gibraltar is facing, the overall understanding of the ML/FT risk is affected by several shortcomings. These shortcomings, include an insufficient understanding of some important threats, including the cross-border threat that Gibraltar faces as an international financial centre, and deficiencies in the analysis and understanding of vulnerabilities, for both ML and FT.

96. Gibraltar demonstrated to have understood, at policy level, the risk posed by tax crimes, as shown by the number of agreements that Gibraltar has signed in past years enabling the exchange of information for tax-enforcement purposes. However, the understanding of ML risk relating to tax crimes, in particular the cross border threat that Gibraltar faces, has not yet percolated down to the GFIU and law enforcement level, as reflected by the poor results concerning the production and use of financial intelligence, in-country investigations and initiatives with regard to MLA concerning ML of tax predicates. This, as described more in detail in the analysis of Gibraltar's understanding of the ML threat, is reflective of insufficient focus on the risk of the proceeds of foreign predicates, particularly financial predicates (for example corruption-related crimes) being laundered through the domestic financial sector and TCSPs.

97. The GFSC and the GGC, as the key supervisory authorities, exhibited a very good understanding of the ML and FT risks, particularly at sector-level. This understanding is underpinned by a variety of data collected by both supervisors. In particular, the GFSC has been collecting financial return data, and since 2016, complemented this data with financial crime returns from the firms subject to its purview. This additional financial crime data is informed by the firms' risk classification of their customers and by several geographic risk-related factors which include, in addition to geographic risk related to customers and BOs, data on cash transactions, as well as inflows and outflows from high risk jurisdictions. Although less granular than the data collected by the GFSC, the GGC also has access to financial return information (such as turnover, margin and gross gambling return) which is used as part of the risk evaluation alongside other return information, such as jurisdictions in which the licensees are active, whether customers from FATF high-risk and monitored customers are accepted, the number of active customers and PEPs and whether any "hits" were identified in respect of targeted financial sanctions (TFS). The other supervisors (for DNFBPs other than TCSPs) particularly the RSC did not exhibit the same level of understanding of the risks posed by their respective sectors, although some of these sectors (for example real estate investment and lawyers and notaries) have been identified by the latest NRA among the highest ML/FT risk areas. Although the understanding of the risk of the OFT is being developed, the OFT has been very proactive in bridging the gap, as, at the time of the onsite visit they were in the process of risk-profiling the firms under their purview.

98. Gibraltar has long-standing experience in ML risk assessment. Prior to 2016, when Gibraltar conducted its first NRA, a national threat assessment was conducted by the GFSC (2012

threat matrix) assessing the products and services which presented a ML risk to the jurisdiction. The 2012 threat matrix included impact and likelihood assessments as well as a threat description, which were shared with the entities subject to the GFSC's purview. The matrix was based on the qualitative data and input of the private sector. Regulated entities (REs) were required to factor this threat matrix into their own risk-based approach (RBA). The threat assessment was subject to frequent updates in order to reflect evolving and new threats in the regulated financial sector.

99. Gibraltar finalised its first NRA in April 2016 (hereinafter: 2016 NRA), using an in-house-developed methodology based on the FATF Guidance – National Money Laundering and Terrorist Financing. The assessment is publicly available in a redacted form. Comprehensive historical data analysis was not available at the time, but a policy decision was taken to adopt the OSCE data model for data collection to support data analysis for future work. The 2016 NRA was therefore prepared using almost exclusively qualitative data obtained from both the private and public sectors and the quantitative data that was available. Representatives of both the public sector³¹ and the private sectors³² (with the exception of lawyers and real estate agents) were involved in this NRA. The 2016 NRA presents “risk events”, assessed in terms of impact and likelihood.

100. The 2016 NRA was complemented by a separate assessment of the FT risk in November 2016 (which assessed the FT risk as low) and by a separate FT risk assessment of the NPO sector (both documents are confidential but the findings were communicated to the relevant stakeholders and to the private sector).

101. In September 2018, Gibraltar adapted the EUSNRA to Gibraltar's framework, assessing the products and services analysis of threats and vulnerabilities in the EUSNRA with the aims of both contextualizing it to Gibraltar and of building on the findings of the 2016 NRA (hereinafter: 2018 NRA). The private sector's involvement was less extensive than in the 2016 NRA, as only trade representative bodies in the finance sector and their member firms were required to provide feedback on an early draft of the 2018 NRA's findings. The 2018 NRA is publicly available.

102. The authorities' efforts to identify, assess and understand the ML/FT risk must be commended. The data collected by the GFSC has constantly improved in the past 3 years and it provides a useful basis for informing the risk supervision of the sectors supervised by the GFSC. The analysis conducted by the GFSC on cash transactions and high-risk jurisdictions can be a valuable tool in the understanding and assessment of the ML and FT threats, both at jurisdiction and sectoral levels. The OFT has been very proactive in developing a more comprehensive understanding of the firms under its purview.

103. The AT is nevertheless of the opinion that several shortcomings affected the overall understanding of risk at country level, particularly the ML risk. This seems to be the due to several factors, including the balance between the qualitative and quantitative inputs during the various exercises (for example, despite the availability of reliable and informative statistics held by the GFSC, the 2018 NRA appears to over-rely on qualitative judgements rather than more objective data) and an excessively top-down approach in the process that, in some instances, may have affected the ownership of and “buy-in” to the end result. As a result, these NRAs do not provide a holistic picture of ML/FT risks present in the jurisdiction and (except in part for FT and some sectoral risks, where the understanding of the risks by some supervisors is good) the ML risk that

³¹ E.g. Attorney General's Chambers, EUID/LSU Finance Centre Director, the GFSC, the Gaming Commissioner; Gibraltar Criminal Intelligence Department; Gibraltar Financial Intelligence Unit; Gibraltar Regulatory Authority; HM Customs and Royal Gibraltar Police.

³² E.g. Association of Trust and Company Managers, Gibraltar Association of Compliance Officers, Gibraltar Banker's Association, Gibraltar Betting and Gaming Association, Gibraltar Chamber of Commerce, Gibraltar Federation of Small Businesses and Gibraltar Society of Accountants).

Gibraltar poses as an international centre is not fully understood, particularly at law enforcement and FIU level.

104. Gibraltar has not conducted a comprehensive assessment of the threats at national level, particularly the cross-border threats to which it is exposed as an international financial centre. Both the 2016 and 2018 NRAs have statistics and charts related to the ML threat (the 2018 having more data than the 2016 NRA), but there is insufficient analysis of this data at country level and limited conclusions are drawn on what types of crimes present the highest threat to Gibraltar. While for the 2016 NRA this could have been in part explained by the more limited statistics available to Gibraltar, during the process that led to the 2018 NRA more data became available³³. Moreover, although the GFSC has been collecting financial crime data (available for 2016, 2017 and 2018) across firms, sectors and products, as well as data for inflows and outflows across a number of sectors, high risk jurisdictions³⁴, and this data could have been used to at least inform the 2018 NRA (particularly since the data from 2016 and 2017 was available when the 2018 NRA was conducted) in fact that data has not informed the 2018 NRA.

105. The insufficient analysis of the threat at country level is particularly relevant for the threat posed by proceeds generated by crimes committed abroad or with a transnational character (such as smuggling and drug trafficking) and, in particular of tax and financial crimes committed in foreign countries. Some elements of cross border threats were considered, for example, the proximity of Gibraltar to organised crime areas, but their assessment produced inconsistent results across the years. Although in the 2012 threat matrix this risk was rated among the higher ones, it is unclear on what basis this factor (proximity to organised crime) was rated as a "minor" risk in the 2016 NRA, when it then rises to 11th out of the 13 higher risks identified in the 2018 NRA.

106. While the 2012 threat matrix assessed the risk of smuggling tobacco, rating it high both in terms of impact and likelihood, and acknowledging the existence of a network of underground connections and systems which supported efficient logistical mechanisms to integrate the cash generated from these activities, the 2016 risk assessments did not sufficiently consider this risk factor (except for the risk of cash that may be associated with the legal trade of tobacco), even though the NRA report and a 2014 OLAF report³⁵ noted an increase in tobacco related offences. The 2018 NRA statistics on investigations into predicate offences corroborate the fact that most frequent local criminal activity is that of theft and smuggling in relation to the export of tobacco products. The risk arising from tobacco smuggling is then only assessed at product level in the assessment of the risk of corporate banking-deposits, where the analysis notes that "*the differential in pricing of tobacco between Gibraltar and Spain and their unique geographical context results in OCGs exploiting this for the illicit trade in tobacco*". In the context of cash couriers / cross border cash movements the analysis shows that the "*Illicit cross border tobacco trading itself generates large volumes of illicit cash. The trade largely conducted on a cash basis therefore bringing large*

³³ The 2016 NRA has some data on STR analysis, European arrest warrants execution, MLA requests, arrests made by Customs; whereby the 2018 NRA has more detailed data on STRs, incoming and outgoing requests handled by law enforcement; FIU exchanges (incoming requests only, but not those outgoing) and MLA (incoming requests only but not outgoing); investigations, prosecutions and convictions for predicate offences, financial sector data, such as active individual customers by country of residence and active corporate clients by country of corporate's activity, with data on geographic risks (including for wire transfers).

³⁴ Together with details of countries of nationality, residency and activity, as whether a PEP/ close associates of a PEP across the same demographic analysis.

³⁵ OLAF expressed a number of concerns "regarding the link between a significant increase in the size of the Gibraltar market for cigarettes over the past four years and the subsequent increase of cigarette smuggling across the frontier and corresponding increase in size of the illicit market in southern Spain". <https://www.telegraph.co.uk/news/worldnews/europe/gibraltar/11026733/Money-laundering-and-smuggling-over-Gibraltar-border-on-the-rise-says-EU.html>

volumes of cash into the financial system that may then be laundered through other methods.” Despite these findings, the assessment rates the risk emanating from tobacco smuggling among the lower categories of risk, which does not seem consistent with the threat analysis.

107. As regards financial crimes, the analysis of the risk of ML related to foreign corruption was almost exclusively driven by an analysis of the level of corruption that may be present in countries close to Gibraltar, and not from an analysis of the financial flows to/from countries at risk of corruption, which may not necessarily be close to Gibraltar.

108. It is commendable that the risk of tax evasion was assessed by both the 2016 and the 2018 NRAs, but there appear to be inconsistencies when comparing the two findings, given that the underlying factors underpinning this risk were almost the same. The 2016 NRA assesses the risk of tax evasion, primarily as related to “tax planning and transactions” (which are rated among the higher risk categories) and noting as a factor the increased likelihood of occurrence of abuse of corporate and legal structures, use of nominee shareholdings, corporate directors and banking facilities for the same, but without analysing whether the tax evasion risk is domestic or external. The same risk category is also analysed in the 2018 NRA, and the same risk increasing factors are noted, but the risk is assessed as low, on the basis of risk-decreasing factors that were also present in 2016 (and that are only based on “presumptions”).³⁶

109. Another risk that does not appear to have been assessed against all available data is the risk related to cash. The 2018 NRA looks at this risk both in terms of cash intensive businesses (which could be used to launder proceeds of crime) and in terms of cash couriers. However, the analysis of cash couriers considers only the threat posed by cash generated by illicit tobacco, and not from other criminal proceeds (e.g. tax crimes) that could be smuggled into Gibraltar. This approach is questionable when looking at the data collected by the GFSC on cash transactions. This data shows an increase, which is particularly relevant in the banking sector, if comparing, for example, data on the average amount of cash transactions between 2016 and 2017³⁷, or if considering the total value of transactions received in cash by the banks in 2017 which is GBP 1,285,986,570³⁸. Having in mind that the majority of customers in the banking industry are non-residents, the conclusion that “there is no evidence of money mules mechanisms in Gibraltar”, which was reached in the 2018NRA in assessing the risks related to the deposits on accounts, can be questioned³⁹. The AT is of the opinion that the explanation given by Gibraltar that most of these cash transactions are related to paying wages to non-resident workers or to the sales of tobacco is not convincing.

110. These deficiencies in the analysis of the threat are compounded by shortcomings in the analysis of the vulnerabilities. There was an insufficient assessment, in both the 2016 and 2018 NRAs of human resources and capacity, in spite of the fact, for example that the statistics presented to the assessment team show that in 25% of cases a financial investigation was not carried out as a result of lack of resources (see IO6). The assessors take the view that both the MLIU and OCP&L are not sufficiently resourced to deal with the investigation and prosecution of ML cases of any significant scale which would be likely to be generated if the AML system was operating effectively

³⁶ “Tax evasion is a serious criminal offence and a predicate offence for the purposes of ML and professionals are aware that suspicious activity in this area is reportable; TCSP, Legal and Accountancy professionals together with Notaries and Tax advisors are relevant financial business under POCA requiring them to have AML/CFT measures in place and are regulated to ensure that these are effective”.

³⁷ The average amount of cash transactions increased from GBP 806 (2016) to GBP 6198 (2017).

³⁸ GFSC financial crime data for the year 2017.

³⁹ This finding is also not supported by the authorities’ analysis of tobacco smuggling, which shows that “*Illicit cross border tobacco trading itself generates large volumes of illicit cash. The trade largely conducted on a cash basis therefore bringing large volumes of cash into the financial system that may then be laundered through other methods.*”

(see IO7). The inherent vulnerability related to Gibraltar's port and to the services provided to ships and vessels was also not analysed. An example noted under the analysis of IO8 is the frequency with which ships and luxury vessels enter the port of Gibraltar to refill their oil tanks.

111. The 2018 NRA top 13 combined ML and FT risks are (in risk-decreasing order): E-money; Conversion of funds; Creation of legal entities and legal arrangements; Retail financial sector-Deposits on accounts; Virtual currencies; Transfers of funds; Cash intensive businesses; Investment real estate; Payment services; Private banking-Deposits on accounts; Proximity to Organised Crime; Legal service from notaries and other independent legal professionals; Sanctions. The AT has reservations about the risk classification of the 2018 NRA and about the quality of the analysis, which is based primarily on products and services without a holistic approach in understanding and assessing the overall risk that a relevant sector, or the jurisdiction as a whole, may face and with a limited contextualization to Gibraltar of the findings of the EUSNRA. For example, online gambling does not appear to be among the highest sector/products identified, although the sector accounts for the highest number of STRs. The authorities explained that this is the outcome of the combined ML and FT risk assessment, but that if looking at the ML risk alone, the sector would score higher. This explanation is not fully convincing, not only because of the materiality of the sector and diversity of customers (including from a geographic risk, given that most of online service providers licensed in Gibraltar provide their services in several countries), but also because there have been cases related to online gambling with proceeds of crime and, as noted under IO9, instances where internet gambling could potentially be used for FT. However, the 2018 NRA has ruled out the FT assessment of online gambling (both in terms of threat and vulnerability).

112. In some other instances the absence of specific data underpinning the analysis of the 2018 NRA makes it challenging to agree or disagree with a particular risk rating: for example in the case of private banking, which was rated 10th (out of 13) is less risky than "Retail financial sector – deposits on accounts" (rated 4th out of 13), without a comparative analysis of data on the number of clients and assets held for each of these two products/services. Moreover, the analysis of private banking (both threat and vulnerability) was taken verbatim from the EUSRA, without any contextualization to Gibraltar. It is also unclear while "legal services provided by notaries and other independent legal professionals would be among the first 13 higher risks (12th out of 13) and riskier than online gambling operators, considering that legal services are less material than online gambling (there are 12 notaries and 39 law firms, out of which only 30, according to the authorities, provide services that would fall under FATF R.22). The analysis in the 2018NRA is again taken verbatim from the EUSRA, without contextualizing to the Gibraltar's framework except for noting that lawyers are regulated by the RSC. In the 2016 NRA the risk related to legal services was rated as medium, but the analysis is the same as the 2018NRA, except that the 2018 NRA assessed the risk related to legal services as higher. Finally, given the relatively small size of the virtual currency sector (see Chapter 1), the existence of market entry controls and AML/CFT requirements and the level of awareness of such requirements and of the risk exhibited by the sector, the assessment team is of the view that the sector may not currently pose a significant ML risk.

113. The analysis of the ML/FT vulnerabilities undertaken by the 2018 NRA is often not comprehensive and is superficially limited to considering that a given product or service is subject to preventive or other regulatory measures⁴⁰.

⁴⁰ For example, the assessment of the ML risk related to private banking (wealth management) "shows that this sector is used in connection with the following predicate offences: corruption and drug trafficking, fraud and tax evasion. This reduces the "scope" of organised crime organisations that may rely on this risk scenario. It requires some level of expertise that makes it not so easy to access and not very attractive (not

114. The assessment team has reservations about the approach taken by the Gibraltar authorities in assessing the risk posed by the banking sector as a whole. Although the misuse of client bank accounts was identified among the higher risks in the 2012 matrix, banking sector and banking products and services were not included in the 2016 NRA and were assessed only as products and services by the 2018 NRA. The assessment team considers this to be insufficient, given the size and materiality of this sector. While the GFSC exhibited a robust understanding of the risk from all sectors, including the banking sector, under its purview, the insufficient assessment of this risk in both NRAs has resulted in the sector being supervised much less compared to other sectors (e.g. the TCSP and e-money sectors, which were both subject to thematic reviews).

115. As specifically regards the assessment of the FT threat and overall risk, the 2016 analysis found that Gibraltar only presented a low to medium risk of FT and that no specific actions were required to be conducted to mitigate the risk. The AT is not in a position to agree or disagree either with this statement or with the conclusion that there were “no indications, therefore, that Gibraltar based providers, products or services had been used as a FT conduit or as a revenue raising jurisdiction” but only because this assessment was based on the analysis of limited data (lacking the following data: FT related STRs, , formal MLA requests from foreign countries on FT related matters, and FIU to FIU or LEA to LEA requests) and not based on statistics of financial inflows and outflows to e.g. high-risk jurisdictions or jurisdictions and areas bordering with such jurisdictions.

116. There are a number of additional issues concerning this FT risk assessment, which have affected the authorities’ understanding of FT risks and prevented them from taking timely measures to mitigate those risks that could have been identified by applying a more rigorous approach. The 2016 standalone FT risk assessment is a list of threat factors taken by FATF studies, with some limited analysis to customize it to the Gibraltar’s framework. The assessment of the effectiveness of risk-mitigating measures is also generic and, at times contradictory. For example, the analysis considers that strict border controls at all entry and exit points, including cash declaration systems in place mitigate the risk of physical cash movements, but this is inconsistent with the statement in the same report that “*HMC is currently developing the cash declaration process at our entry and exit points*”, and with the fact that cash declarations were implemented only in 2018 (after the FT assessment was finalized). As noted in the analysis of IO8, the AT has reservations about the effectiveness of cash declarations, particularly if one considers the amount and overall value of cash transactions conducted in the banking sector alone.

117. It is commendable that in the 2018 NRA products and services were also assessed for FT risk, and the assessment was that Gibraltar had to be cognisant of its role in attracting international financial services and products and how these might be attractive to terrorist financiers. The following products/areas were identified as posing a higher FT risk on a scale from 0-8 (threat and vulnerabilities, from lower to higher): e-money (8), transfer of funds and sanctions (6), payment services (5), deposits on account, creation of legal persons and arrangements, cash

financially viable). In particular, when dealing with private banking, the service is quite “high cost” (need of sufficient funds to access this financial service) and the business relationship less easy to establish.” For corporate banking deposits on accounts the analysis of the vulnerability notes that “The majority of corporate entities in Gibraltar are managed by a TCSP. Therefore, there is an increased level of awareness and controls in place to reduce the vulnerability of misuse of bank accounts for ML from cash fronted businesses. This is due to transaction monitoring being a requirement to be conducted by both the TCSPs and FIs, which should flag any instances of ML” carried out by a local entity. However, the thematic inspections of the TCSP sector (conducted by the GFSC as a result of the 2016 NRA) shows several issues related to the effective implementation of AML requirements.

intensive business, investment in real estate, services from independent legal professionals and virtual currencies (4). The AT agrees in general with this risk classification but, as for the 2016 FT standalone risk assessment notes that the analysis of cash couriers (which was given a rating of 2) is not consistent with the data on cash transactions. The analysis of this data, and the very recent implementation of cash declarations, could warrant, when comprehensively analysed, a different risk rating for cash couriers⁴¹.

118. This insufficient understanding of FT risk at country level is, in part, mitigated by the better understanding of FT risk demonstrated by the GFSC. The GFSC further conducted a study of transactions from/to conflict zones, based on 2016, 2017 and 2018 data, which is well researched. The analysis of 2016 data shows that out of 43,6 mil. transactions, 5,6 mil transactions were made to high-risk jurisdictions. The analysis of the 2017 data is more detailed and shows that the absence of any FT related SARs submitted by banks against the backdrop of over 30,000 transactions linked to the high risk countries (approximately 80,000 including the Drug transit/producing countries) could potentially raise some concern, and at the very least, warrants some further investigation. The study shows also a vulnerability to FT for the e-money and TCSP sectors. The 2017 data shows, among the recipient countries, several that are conflict countries or close to conflict countries or with high risk of terrorism. Similar trends can be observed for the transfers done in 2018 (please also see paragraph 274 under IO9). Although these analyses were forwarded to the NCO and the GFIU they did not warrant further mitigating measures in the action plans or a re-assessment of the FT risk.

2.2.2. National policies to address identified ML/FT risks

119. Following the publication of the 2016 NRA, an Action Plan (2016 Action Plan) was designed and put into effect in December 2016 with specific risk mitigation measures for each of the risks identified by the April 2016 NRA, with a timeframe for completing the relevant actions spanning until June 2018. While several actions appear appropriate to mitigate the identified risks, the issues noted with regard to the proper assessment and understanding of certain factors and risks has affected the comprehensiveness of the action plan and the capacity of the measures envisaged by the plan to actually address the risks in an effective manner. This is of particular concern for the risks related to Gibraltar's proximity to organised crime, which was deemed as "low" priority; the one related to sanctions, which was deemed as "medium" priority, in spite of the gaps existing in Gibraltar's legal framework at that time for the implementation of TFS. The lack of assessment of the banking sector, or banking products and services (which was done only in the 2018 NRA) resulted in no actions being identified at country level for this sector (the GFSC focused on thematic reviews of e-money providers and TCSPs, while some of the banks interviewed by the team had not been inspected for AML/CFT compliance by the GFSC for some years).

120. No specific measures or actions were identified to mitigate the risks acknowledged by the November 2016 FT NRA (except for recommended actions related to the vulnerabilities identified in the 2017 risk assessment of the NPOs).

121. The 2016 Action Plan includes measures aimed at a more effective use of resources based on risk (e.g. for the GFSC to enhance the RBA supervision and the GCID to focus resources on high-risk individuals involved in organised crime). The assessment team welcomes these measures but also notes that, at the time of the onsite visit, issues concerning human resources were still affecting LEAs' efforts (see IO7)

⁴¹ The overall value of transactions paid out in cash by the banking sector only, during 2017 was GBP 458,285,724

122. In April 2017 Gibraltar adopted an AML/CFT strategy which outlines high-level strategic outcomes (prevention, detection, enforcement, international and awareness), with specific actions for attaining them. The strategy appears to be open ended and is complemented by specific action points and outcomes to achieve but, unlike the 2016 NRA action plan, there are no specific deadlines for the achievement of the outcomes. The authorities stated that the strategy is informed by the risks identified by the 2016 NRA, as well as by the FT risks identified by the FT and NPO risk assessments. The strategy and the action points were also complemented by ad hoc measures, such as a recent decision to increase the workforce of the Royal Gibraltar Police (RGP) over a three-year programme, which occurred after the onsite visit: this is a very positive development, given the concerns expressed by the AT (see analysis of IO6 and IO7, noting capacity/resources issues for the RGP and the prosecution). There are some areas for improvement in the action points, particularly in regard to the Customs' capacity to detect cash smuggling more effectively and to prevent the continuous turnover of seconded staff of the GFIU (see analysis of IO6).

123. There are FT-related strategic documents that provide a number of legal and operational measures, including a document that sets out the arrangements in place for the collection, gathering, governance, responsibility and operation of the LEAs and supervisory bodies with responsibilities for CFT. Whilst this is commendable, the authorities would benefit from a more unified strategy targeting specific risks in Gibraltar and identifying and developing any typologies observed, as noted under IO9.

124. The authorities stated that there are no immediate plans to revise the current strategy in light of the revised 2018 NRA because, after having reviewed it and resulting action points and they are of the view that as the strategy remains relevant.

125. However the full relevancy of the 2017 strategy can be questioned, given the increase in the risk identified in certain areas between the 2016 and the 2018 NRAs (for example the proximity to organised crime) and the fact that new risks were identified, which were not identified in the 2016 NRA (e.g. the use of products in the banking sector, cash intensive businesses.) The current strategy does not appear to tackle these effectively. The insufficient understanding of the risk posed by cash has also resulted in this risk not being sufficiently addressed by the strategy and any action points.

126. Most of the measures envisaged by the action plans and strategy were implemented by the authorities, with some exceptions such as, inter alia, in the case of measures to prevent the use of anonymous pre-paid phone cards (identified as being exposed to FT risk); and requirements for real estate agents to produce audited accounts on an annual basis and ML/FT risk scoring for such agents (which is not yet fully operationalized to drive supervision of this sector based on its risk). The 2017 data analysis of transactions with conflict zones and high risk jurisdictions envisaged that there would be targeted onsite inspection visits to be undertaken in the banks and e-money firms that reported a link to the high-risk countries to test the following controls specific to sanctions screening, enhanced CDD, transaction monitoring and SARs reporting process; however only e-money firms and TCSPs (and not banks) were subject to a thematic review. The thematic review of the TCSP sector from 2018 noted certain shortcomings, which, although not endemic to all firms, were an area of concern for many of them (please see paragraphs 273-274 under IO9). Whilst the GFSC is to be commended for the work done in the afore-mentioned analysis it remains unclear why the conclusions and recommendations provided therein did not trigger additional mitigating measures in the action plans. It is also unclear why the thematic reviews conducted by the GFSC did not focus on the SAR reporting process, although the GFSC had expressed concern about the low number of SARs related to FT vis-a-vis the number of transactions to/from conflict zones.

2.2.3. Exemptions, enhanced and simplified measures

127. There are a number of exemptions which are not based on verified low risk or justified by the results of the risk assessments (see R1). Situations requiring enhanced and simplified CDD mirror those envisaged by the 4th EU Directive but are not based on an actual assessment of risk. While some of the exemptions may not have a significant impact, the AT team has some reservations about those that were allowed for some entities which were identified as higher risk by the NRA (SCDD for lawyers, which exempts from the identification of the BO and from carrying out on-going monitoring) or those that are concerned with the identification of a customer that is a FI in Gibraltar or in a EU country, or, in the case of the beneficiaries of a trust, limit the definition of the BO to those owning 25% or more of the assets within the trust⁴².

128. Although the NRAs identified specific high-risk areas for ML (e.g. tax planning structures and transactions; real estate, securities and funds sector) and FT (e.g. virtual currencies and pre-paid cards), and the law provides for the Minister to rule on additional situations requiring ECDD, no such determination was taken.

2.2.4. Objectives and activities of competent authorities

129. The GFSC's objectives and activities are, in part, aligned to the risks identified by the NRAs, and by its own understanding of risk, although the lack of assessment of the banking sector (and its product and services) in the 2016 NRA, and the issues noted in the assessment of inherent vulnerabilities by the 2 NRAs, has resulted in this sector being inspected with less frequency than other sectors (such as the e-money firms, which together with TCSPs were subject to thematic reviews following the completion of the NRAs), despite its materiality and inherent risk.

130. The GGC objectives and activities are consistent with their understanding of the risk posed, particularly by those risks associated with remote gambling as identified by the 2018 NRA, although they were neither aware of the detailed analysis of the 2016 NRA concerning this sector nor of the follow-up actions that had then been envisaged. As regards the other supervisors, their responsibilities were only recently assigned to them and their activities were not yet fully informed by the risks identified by the NRA, although, in the case of the OFT, the AT noted on-going progress in bridging the gaps.

131. The GFIU does not prioritise its objectives and activities in a way that is commensurate with the risks that Gibraltar is facing as an international financial centre. So far, no strategic

⁴² Firms are not required to verify identity in the case of public listed companies admitted to trading on a regulated market within the meaning of Directive 2014/65/EU in one or more Member States and listed companies from third countries which are subject to disclosure requirements consistent with Community legislation (6.2.1.2.1., in these cases FATF only exempts from the verification of the shareholders or beneficial owner's identity, not of the company's) or when there are reasonable grounds for believing that the applicant for business is itself a financial institution in Gibraltar or an EU country (6.2.1.2.2). The GFSC AML/CFT Guidance Notes (7.2.2.) also exempt verification in "exceptional circumstances", when applicants for business will not be able to provide appropriate documentary evidence of their identity and where independent address verification is impossible. In such cases, firms might agree that a senior manager may authorise the business if he/she is satisfied as to the applicant's acceptability. In case of SDD, RSC Guidance mentions that a legal professional is not required to obtain information on the nature and purpose of the business relationship or on beneficial owners, and it is implied that neither on-going monitoring is not required. Legal professionals need only obtain evidence that the client or products are eligible for SDD (Section 4.8.1, RSC guidance). The definition of beneficial owner adopted by the GFSC GN in the case of trusts limits the term, in the case of beneficiaries, to those that own 25% or more of the assets within the trusts. Finally, the exemption on the application of correspondent banking requirements to EEA-based is also not based on an actual risk assessment, but on presumptions.

analysis of transactions flows to identify typologies related to foreign predicates and the risk related to the misuse of complex corporate vehicles has been developed by the GFIU.

132. Law enforcement authorities mainly focus on fraud, drug trafficking, smuggling and services such as e-money, real estate, and cash-based retailers. The LEAs' efforts, however, appear not to be commensurate with the ML risk emanating from other types of offending, especially from tax crimes committed abroad, whose proceeds may be laundered in or through Gibraltar. This is also evidenced by the statistics on MLA, which are not commensurate with such risks.

2.2.5. National coordination and cooperation

133. Cooperation and coordination among stakeholders are effective and are one of the strengths of the jurisdiction. Through the office of the NCO and the Interagency Working Group, in which all main stakeholders are represented, all policy and operational matters are co-ordinated and discussed to give effect to the desired outcomes. The Group is composed of the representatives of the following institutions: GFSC, GFIU, RGP, GLO, HMC, GCID, ITO, OFT, GGC and Gibraltar Court Services, and, as per its ToRs, discusses the following matters: i) Financial Crime Trends; ii) Operational Challenges; iii) Deficiencies in the current Law; iv) MONEYVAL and any other evaluations; v) The best use of resources; vi) On-going investigations and vii) Training Programme. Additionally, ad-hoc meetings take place between the NCO and stakeholder authorities as well as between authorities themselves outside of formal groupings to ensure co-operation.

134. During the interviews held on-site all representatives of the institutions concerned expressed their support to the way the Group operates. They also emphasised the added value it brought in fostering inter-institutional cooperation. As an example, GGC underlined the closer cooperation with the GFIU which in the past was mostly limited to the exchange of intelligence. The GFSC also confirmed that the exchange of information had intensified since the Group was established. The GFSC is now consulted on operational matters mostly in cases when a RE which is under their supervision is a source of in a ML/FT or predicate offence investigation. The 2017 Strategy acknowledges the NCO's role in ensuring a strategic and proactive approach to the development of policy, legislative as well as workflows to improve the AML/CFT regime. In order to provide a more formalised support for the NCO, the strategy had also envisaged that HMGoG would have established a formal Steering Committee structure where all policy, legislative and workflows would be discussed, and recommendations made to HMGoG for their attention and action as necessary. However, the Steering Committee was not in place at the time of the onsite visit.

135. At the operational level the Group discusses AML/CFT matters arising from different ML/FT or predicate offence investigations. RGP⁴³ and HMC as key LEAs in Gibraltar are actively engaged not only in the Inter-agency Working Group but also in numerous ad-hoc arrangements aimed at tackling particular economic crime. As an example, RGP presented the recently signed MoU ('Agreement on Joint Task Force for Operation Fusion' – discussed also under IO6) by RGP, HMC, GFSC and the Tax Office. The MoU and all the signatories committed to disseminate appropriate intelligence to each other, ensuring the protection and confidentiality of data.

136. With regard to FT related matters the GFIU and the RGP maintain links with the NTFIU which is part of the UK's Metropolitan Police. RGP Special Branch which is in charge for CT investigations is in permanent communication with the RGP's ECU and GFIU ensuring coordination and information exchange with regard to CT and FT related matters.

⁴³ These LEAs, in their Standard Operation Procedure, which sets up 'take on' criteria when investigating ML, requires officers to examine the alleged crime 'correlation with the NRA'.

137. In addition to effective multi-agency cooperation at the national level, the authorities take part in numerous international platforms which discuss operational and other matters related to AML/CFT (Egmont, CARIN, Interpol, etc.). Nonetheless, Gibraltar LEAs have not yet been a part of any international joint investigative team, although the legal framework is in place to support such cooperation.

138. A legal basis exists in the NCOR and POCA as well as the FS(IG&C)A to permit a free exchange of relevant information between all stakeholder authorities. Nonetheless, to further strengthen the exchange of information, numerous MoUs were signed (i.e. MoU between OFT and GFIU; MoU between RFS and GFIU; MoU between ITO and GFIU and MoU between GD and GFIU). In particular, the MoUs aim to facilitate further working relationships among parties concerned and increase communication fluidity and data protection. In addition, each party committed to assign a point of contact for information exchange. Whilst the authorities are aware that effective inter-agency cooperation could have been executed even without formal MoUs, they advised that further formalisation of cooperation and especially the appointment of contact points through these agreements brings more tangible results.

139. There is little evidence of any co-ordination or discussion by the Inter-agency Working Group in relation to PF matters. Accordingly, it remains unclear whether the level of co-ordination, cooperation and sharing of information and intelligence across all relevant sectors is adequate to effectively combat PF.

2.2.6. Private sector's awareness of risks

140. A redacted version of the 2016 NRA and the full version of the 2018NRA are publicly available. Several efforts were made to make FIs and DNFBPs aware of the findings of the FT and NPOs NRAs, as well as the main findings of the 2016 and 2018 NRAs, particularly through Project Nexus, which was developed as an outreach programme initiative aimed at providing AML/CFT awareness and other relevant presentations to REs. Specific NRA outreach programmes were delivered across all institutions and specific industry sectors (e.g. banking, TCSP, and the legal profession, as well as compliance officers and risk managers). However, the understanding of the results of the NRA and, in general, of the ML and FT risks by FIs and DNFBPs was almost exclusively related to the 2018 NRA, and with varying degrees of awareness (see analysis of IO4). REs were not always aware of the FT and NPOs risk assessments, despite these being relatively recent. Some types of FIs (e.g. fund managers, DLT providers and electronic money and bureaux de change) demonstrated overall a good understanding of their ML and FT risks. Among DNFBPs, TCSPs and online gambling providers had a good understanding of the ML/FT risks that they are facing. However, the AT is concerned that the TCSPs industry association was not aware of the 2018 NRA findings and of the other risk assessments, and appeared to not fully understand the risk that this sector is facing.

Overall conclusions on IO.1

141. Gibraltar is rated as having a moderate level of effectiveness for IO.1.

3. LEGAL SYSTEM AND OPERATIONAL ISSUES

3.1. Key Findings and Recommended Actions

Key Findings

Immediate Outcome 6

- a) The GFIU has increased its capacities in recent years, including its human and IT resources, but further improvement is needed for both elements. The GFIU has also extended cooperation with the LEAs and supervisory authorities, thus increasing its role in generating financial intelligence. The GFIU's analytical products were used by LEAs only to a limited extent and therefore did not have a significant impact upon developing investigations into ML and predicate offences. Somewhat better results were achieved with regard to FT investigations. The statistics and cases examined confirm that the overall use of financial intelligence and other relevant information by LEAs to develop evidence related to ML, FT and predicate offences is insufficient relative to the risk and context of the jurisdiction.
- b) The statistical data on the number of information requests sent by the LEAs to the GFIU, together with the case examples presented, confirm that cooperation and information exchange is conducted on a regular basis. The size of the jurisdiction allows prompt information exchange and consultations among the relevant authorities. This notwithstanding, the disseminations submitted by the GFIU did not assist LEAs, to a satisfactory extent, to perform their duties. This is also a consequence of the fact that LEAs did not prioritise cases concerned with the GFIU disseminations in their work.
- c) The STRs which the GFIU receives are not of sufficient quality to assist them in performing their functions. Partly this is a consequence of defensive reporting which appears to predominate in some sectors (e.g. gambling). Whilst the authorities argued that quantity and quality of reporting from some of the DNFBPs has increased, more efforts need to be invested in improving the quality of obliged entities' reporting. The promptness and frequency of reporting by some sectors also needs to be addressed given the nature of their businesses, the fact that they are operating in an international finance centre and are exposed to a higher ML risk.
- d) Whilst no typology specifically tailored for Gibraltar has been produced so far, the authorities have developed one strategic analysis. This strategic analysis was not made available either to the oversight and supervisory agencies (GFSC, GGC) or to the private sector.
- e) Specific protective measures are in place to ensure the confidentiality of information exchanged, accessed or used.

Immediate Outcome 7

- a) Since 2015 Gibraltar's AML/CFT legal framework has improved significantly. This framework, deriving from the legislation in England and Wales, provides a solid basis for the authorities to detect, investigate and prosecute the ML/FT offence. Whilst this was followed by improvements in inter-agency cooperation and information exchange, the effective investigation and prosecution of ML offences remain undemonstrated.
- b) By the time of the on-site visit there have only been 4 ML convictions, and all are for the self-laundering of domestic predicates. There have been no successful third party and standalone prosecutions over the relevant period indicating that insufficient emphasis is placed by the LEAs on the detection, investigation and prosecution of cases potentially involving Gibraltar's financial

institutions (FIs) and intermediaries, targeting criminal property deriving from foreign predicates (including foreign fiscal predicates). ML investigations into third party ML and leading to standalone ML prosecutions do not appear to have been a key objective for the LEAs and prosecuting authority in the past.

c) The authorities do not develop the intelligence from incoming mutual legal assistance (and other foreign jurisdiction requests) to trigger investigations into potential ML in Gibraltar of criminal property from foreign predicates.

d) Financial investigations are conducted regularly but these are often limited to providing further evidence in support of the prosecution of domestic predicate crime or pursuant to possible confiscation proceedings. Parallel financial investigations targeting ML are not pursued in cases where the associated predicate offences occur outside Gibraltar, thus not reflecting the risks the jurisdiction has in its role as an international financial centre.

e) The law enforcement and prosecuting authorities responsible for the detection, investigation and prosecution of ML are highly motivated to investigate and prosecute domestic proceed generating crime but have insufficient resources to conduct major ML investigations.

f) Gibraltar's independent judiciary does not encounter many ML cases because there are so few ML prosecutions. The judiciary applies the guidance of the sentencing guidelines council of England and Wales and the principles underpinning the sanctioning regime are well developed. The judiciary also confirmed that they were entitled to depart from the guidelines and might, for example, impose higher sentences where the offending might have a tendency to undermine confidence in Gibraltar as a financial centre.

Immediate Outcome 8

a) Gibraltar's legislation provides all that is necessary for the detection, restraint and confiscation of the proceeds and forfeiture of the instrumentalities of crime, whether from domestic or international offending. It also provides non-conviction based civil recovery and cash seizure regimes as an alternative means of disrupting economic crime.

b) Although confiscation is a policy objective, it has not been effectively pursued and the amount confiscated is low. There have been only 2⁴⁴ POCA conviction-based confiscation orders and these arose from crimes committed in Gibraltar. In addition, forfeitures (under the 1997 Tobacco Act) of tobacco and the instrumentalities used to smuggle it (e.g. vehicles and vessels) were applied by HMC throughout the reporting period.

c) Whilst LEAs regularly receive training on financial investigations, have access to a number of databases and coordinate their actions accordingly, the focus is still on the confiscation of the proceeds of domestic predicate crime.

d) Assets deriving from foreign predicates (including foreign fiscal predicates) in complex and international cases remain undetected and therefore the benefit of that crime is neither restrained nor confiscated. This does not reflect the risks faced by Gibraltar as a financial centre.

e) Whilst LEAs have achieved results from cash seizures, the civil recovery regime has, so far, not been applied.

f) The statistics on the confiscation of cross border movements of currency and BNIs suggest that this element in the overall confiscation regime has been underused. The assessment team is of the opinion that a more in-depth analysis of the risks posed by the cross-border movement of cash

⁴⁴ As noted in the text of IO8 a third confiscation order was rendered a month after the on-site.

is needed since the results of the seizure/confiscation of cash/BNIs transported across borders is only partially in line with the risks.

Recommended Actions

Immediate Outcome 6

- a) The GFIU should carry out a review of the use of its analytical products by LEAs and based on this review streamline the intelligence gathering and subsequent reporting to LEAs with a view to improving the relevance of and impact of its products for triggering ML investigations.
- b) Given the jurisdiction's risk profile, the GFIU's and LEAs' expertise as well as the already established inter-agency cooperation should be further developed to be able to focus more effectively on the sophisticated forms of ML in Gibraltar where predicates have been committed abroad.
- c) Gibraltar should carry out sector specific analysis aimed at providing and implementing concrete measures addressing the defensive reporting by the gaming, TCSP and banking sectors. These measures should tackle the need for prompt and higher quality reporting by these sectors.
- d) The GFIU should enhance its capacities in producing strategic and operational analysis, in particular through the development of a handbook to be used by its staff. This would partially mitigate the loss of institutional memory arising from frequent changes of staff. The GFIU should also formulate, from the disclosures received (both from REs and foreign counterparts) ML typologies typically encountered in Gibraltar which would enable both the GFIU and the LEAs to streamline their efforts and better deploy available resources.
- e) Regular outreach programmes (such as project 'Nexus') to the relevant authorities and the private sector need to include the strategic analysis developed by the GFIU.
- f) Further improvements in the GFIU's specialist software are required, particularly the analytical software program.

Immediate Outcome 7

- a) The Gibraltar LEAs should refine and apply a clear policy/strategy on ML investigations, setting out the range of circumstances in which a ML investigation should be commenced which reflects the risks of ML in Gibraltar, paying particular attention to the laundering of criminal property by elements within the financial sector and deriving from foreign predicates.
- b) The MLIU should treat each incoming MLA request in conjunction with the GFIU and with advice from the OCP&L as valuable intelligence that might be developed into a Gibraltar ML investigation, particularly into the possible ML by Gibraltar intermediaries and FIs.
- c) Gibraltar should consider increasing the resources of the MLIU and the OCP&L to add a number of experienced officers, an experienced prosecutor who specialises in financial crime and further forensic accountancy resources to enable complex ML investigations and prosecutions to be undertaken which are in line with the risks which the jurisdiction faces.
- d) The LEAs with the assistance of advice from the OCP& L should pursue more investigative opportunities to address the position where complex legal structures are abused in ML schemes – particularly where the proceeds derive from foreign predicates and there may be difficulties in proving that the property concerned is criminal property. Both the LEAs and prosecutors should consider whether there would be a benefit to more training on the criminal liability of legal entities.

e) The LEAs and prosecutors should make better use of other criminal justice measures (such as civil recovery) where it is not possible to secure a ML conviction. Attendance at a training programme on civil recovery for LEAs and prosecutors would be of benefit.

Immediate Outcome 8

a) Ensure that LEAs consistently carry out parallel financial investigations aimed at the detection of criminal property laundered in Gibraltar and that the results achieved are commensurate with the risk and context of Gibraltar.

b) Gibraltar should make additional efforts to better use the already established channels of international cooperation with the aim of identifying, seizing and confiscating foreign criminal assets located in Gibraltar. The authorities should be more active in searching for assets moved abroad.

c) Develop a financial investigation manual for the LEAs which would include a modus operandi and best practices on search, seizure and confiscation of the proceeds of crime, for all of the types of confiscation available in Gibraltar - conviction based, cash seizure and civil recovery.

d) HMC should systematically apply its powers to detain falsely declared or undeclared cash or BNIs in order to determine whether there is a link with ML/FT or the associate predicate offences and sufficient grounds for a subsequent forfeiture.

142. The relevant Immediate Outcomes considered and assessed in this chapter are IO.6-8. The Recommendations relevant for the assessment of effectiveness under this section are R.1, R. 3, R.4 and R.29-32.

3.2. Immediate Outcome 6 (Financial Intelligence ML/FT)

3.2.1. Use of financial intelligence and other information

143. Gibraltar's law enforcement and other authorities use (to a limited extent) financial intelligence and other relevant information to identify and investigate potential ML/FT and associated predicate offences, to develop evidence and to search for the proceeds of crime. Although the role of the GFIU is well understood by the institutions which primarily use its products, the financial intelligence provided to the LEAs by the GFIU to date did not have a significant impact upon developing investigations into ML and predicate offences. Somewhat better results were achieved with regard to FT investigations (please see IO9).

144. This conclusion has been reached following the assessment team's review of relevant statistics, from considering case studies presented and from discussions with LEAs, the GFIU, the prosecuting authority and a wide range of REs.

145. The GFIU disseminates intelligence reports to a number of institutions, such as the RGP, HMC (the key law enforcement agencies in Gibraltar) and to oversight and supervisory agencies (GFSC, GGC). The reports submitted to the supervisory authorities are aimed at further enhancing the effectiveness of supervision over different categories of entities and to help further in developing the RBA. Since January 2019, a system of submission of STRs ('Themis') has been established, enabling the online submission of STRs by REs. In previous years, reporting was done in writing and then the GFIU staff would integrate these reports into their electronic database which was IBM iBase. Now when a STR is sent via Themis, the system uses a matrix which automatically shows the next steps to be taken by the GFIU analyst.

146. To perform verifications on the history of persons mentioned in a STR or other available data, the GFIU currently uses both IBM iBase and Themis. System searches are manual in IBM iBase

and partially automated in Themis. In cases where a STR is linked to a PEP, the system automatically recognizes that and marks such a STR as a priority. The same applies to STRs associated with FT and related international sanctions, transactions involving high risk countries and cases where there is a possibility of blocking transactions and freezing funds.

147. The GFIU has direct access or access upon request to the following databases/information sources: Police Databases (e.g. previous convictions), INTERPOL (eASF and FTF database), GCID (Network of foreign LEAs), HMC, NCA UK, HMRC UK, Egmont, Companies House, UBO Register, Motor Vehicle Database, Border Management System (NSCIS), Advance Passenger information (NSCIS), Tax Office, Employment Database, Vessel Registration (Port Authority), Land Property register, Aquagib/ Gibelec – Utilities, GFSC, Gibraltar Finance Department, CS&RO (Identity Cards/ passports etc.), Borders & Coastguard Agency (BCA), World Check, Sanctions Lists, C6 (Acuris Risk Intelligence). These databases are regularly checked against a person(s) subject to the STR(s) received. Overall both LEAs and the GFIU regularly explore data available through these databases. Given the risks and context of the jurisdiction, the assessment team is of the opinion that these databases provide a sound basis in gathering the information the LEAs and the GFIU need.

148. If a case is related to a foreign country (or countries), the information/financial intelligence is sought through the GFIU which then uses its channels (including the Egmont network) to obtain the required data.

149. The LEAs also use other relevant platforms, such as the CARIN network and a network of liaison officers to obtain information which would help them in on-going investigations when seeking evidence or tracing assets. Both the RGP and HMC, while carrying out a financial investigation, collect information and data from different sources/databases. For this purpose a specific checklist⁴⁵ was developed which includes all databases where relevant information is to be sought. It is mandatory for each financial investigation to make these checks. For the RGP the following intelligence can be obtained directly or through the submission of a Data Request without a Court Order: Land Property Services (property ownership); Motor vehicle licensing; Port authority (for leisure boats/crafts); AquaGib/Gibelec (Utilities) and the Gibraltar Maritime Authority (Yachts and larger ships). Whilst the Economic Crime Unit of the RGP has direct access to the Companies House database, the information from the UBO register is obtained through the GFIU (in the form of intelligence).

150. The authorities presented statistics on the disseminations and financial intelligence reports produced by the GFIU and their usefulness to the LEAs. The table below reveals that in the period 2014-2018 a total of 269 intelligence reports were disseminated to LEAs. The figures for investigations triggered by these reports were low: out of the 269 intelligence reports disseminated to the LEAs, only 10 resulted in a ML related investigation. All these investigations were initiated by the RGP - five of them had drug trafficking as a predicate crime, three were related to smuggling and two to fraud. One dissemination resulted in a cash seizure⁴⁶. More importantly, only one of these investigations reached the prosecution phase. The RGP did not initiate any predicate offence investigation based on intelligence reports received from the GFIU. HMC commences, *ex officio*, a financial investigation as a result of receiving a GFIU intelligence report. By the time of the on-site visit none of these investigations had been completed. The proportion of GFIU disseminations leading to FT investigations is greater than those leading to ML investigations. FT related intelligence is of use to LEAs in initiating FT investigations. Out of 55 FT STRs received, 16 disseminations were sent to LEAs which triggered 14 investigations (see table

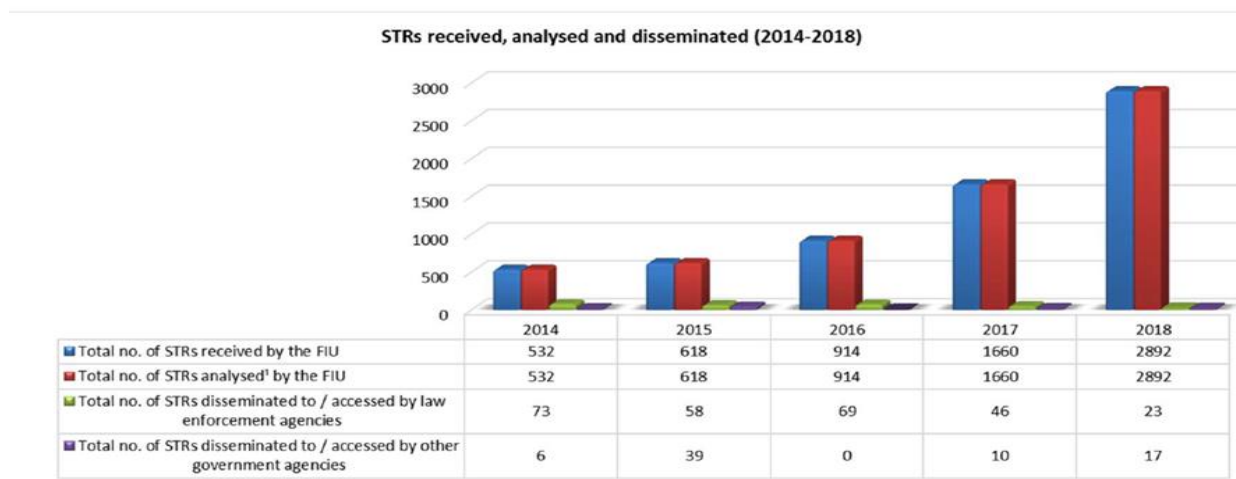
⁴⁵ The checklist, including databases which are looked into by LEAs is covered in more detail under I08.

⁴⁶ Please see para 224 under I08 which elaborates further on cash seizures.

7). None of these resulted in a prosecution but in each case the GFIU duly disseminated intelligence to the UK and any other relevant jurisdiction.

151. The majority of ML and predicate offence investigations were prompted by the LEA using initial information/intelligence from its own sources (i.e. ‘other relevant information’ as referred under core issue 6.1). This mainly consisted of (i) information gathered from a financial investigation following a drugs seizure, (ii) information received from police networks (Interpol, Europol and through bilateral contacts), (iii) information received from informants, from citizens (on fraud cases mostly), from the media and (iv) upon the detection of cash. Both the RGP and HMC confirmed that whenever they initiated investigations or pre-investigations related to potential ML activity (including cash detection), they informed the GFIU. In the period 2016-2018 statistics provided by the authorities show that 51 ML related investigations were initiated. 10 of these were triggered by a STRs/intelligence reports from the GFIU, the remaining 80% (approximately) of ML related investigations were prompted by the LEAs’ own sources. There are considerably more investigations into predicate offences⁴⁷ than parallel investigations into the ML of the proceeds of that predicate criminality: of the 122 investigations on drug trafficking (2016-2018) only 29 prompted ML investigations and of the 107 investigations on smuggling only 4 generated ML investigations. The authorities advanced that this shortfall between the investigation of predicate crime and the investigation of the ML of the proceeds of that crime was for a number of reasons: in most cases the benefits obtained/attempted to be obtained were insignificant; no property may have been found to have been in the suspect’s possession, there were therefore no assets to seize and no ML charges followed⁴⁸. Also, the statistics presented to the assessment team show that in 25% of cases a financial investigation was not carried out as a result of lack of resources (see also Table 18 under IO8). Whilst it is beyond the reach of the assessment team to determine whether the explanations provided by the authorities fully account for the afore-mentioned shortfall, further efforts are needed from the authorities to ensure that ML investigations and confiscation opportunities are systematically pursued.

Table 11: STRs Received, analysed and disseminated (2014-2018)



152. In addition to the submission of initial intelligence reports, the interaction between the GFIU and the LEAs is extensive. The GFIU provides the following assistance in the course of the RGP’s or HMC’s financial investigations: any information available to them about the suspect; whether the suspect was the subject of any STR received; ‘financial profiling’ of the suspect; and provision of in-house expertise in analysing financial records. The assessment team was satisfied

⁴⁷ Majority of predicate offences include theft/robbery, smuggling and drug trafficking.

⁴⁸ For further explanation on the reasoning as to why ML charges and confiscation of assets were rather rarely applied please also see paragraph 200 under IO7.

that inter-agency cooperation was smooth and no impediments to information exchange or any other aspect of cooperation were observed.

153. Since 2015, the GFIU has received 111 requests for information from LEAs. All these requests received a prompt response. In receipt of the LEA's request, the GFIU might then in turn request data from the REs, regardless of whether the RE had previously submitted a STR. To do this, the GFIU gathers further information using the exemptions provided under the DPA which provides exemptions enabling the release of data when it is for the purposes of assisting a LEA with an investigation. In December 2016, amendments to the POCA saw the introduction of a GFIU power to request further (defined) information (for intelligence purposes only) from the RE which may be needed as a result of any report received by the GFIU (and not necessarily a STR). These amendments made it an offence to fail to comply with any such request. Such requests are mostly sent to banks and typically require information about the following matters: (i) bank accounts; (ii) CDD documents; (iii) transaction details including specific dates and times of withdrawals; (iv) outgoing international transaction details; (v) confirmation of any relationship (if any) between subjects and whether they hold accounts jointly; (vi) transactions in respect of specific corporate structures and/or subjects within client accounts; and (vii) a list of companies associated with a subject and managed by a TCSP. The authorities could not provide exact figures for how many times this power had been used but from the cases discussed it appears that it has not been frequently used until recently. Gibraltar's LEAs may apply to the court for a production order to gather further evidence. Foreign LEAs use the MLA/ILOR channels for the same purpose.

BOX 1 - CASE STUDIES

Op Cherokee

This is an on-going RGP investigation into self & third-party ML. Information had been received from French authorities and media outlets. The French authorities initiated the investigation. The original suspicion was that the subject had received/been given state funds to leave Syria after he attempted an unsuccessful coup. The subject had been charged in June 2016 with embezzlement of public funds, laundering as an organised gang and undeclared labour. French intelligence stated that there were huge discrepancies between his asset/resources and his expenses. Subsequent STRs and intelligence packages from the GFIU assisted police investigators. The GFIU looked into whether a subject and/or known associates had (i) ties to locally registered companies; and (ii) bank accounts held within the jurisdiction.

Searches of the company and UBO register were conducted and various Gibraltar registered companies both live and closed were identified as owned in whole or part by the subject or known associates. Some of the companies identified were owned by other companies from jurisdictions outside of Gibraltar. Both live and closed bank accounts were identified, and the GFIU placed a No Consent Order on these accounts.

A search for properties/assets held in Gibraltar was conducted and various apartments, parking spaces and a building were identified. GFIU obtained a valuation of the building held by the subject in preparation for any future confiscation order which might take place.

Further information regarding the Ultimate Beneficial Owner (UBO) of these companies was sent to the countries where the identified parent companies were located. Egmont Intelligence Reports were forwarded to the French and UK FIUs. GFIU 1D powers were used to request further information including bank account statements and mandates.

Cash seizure (international enquiries and sharing of intelligence)

EUR 7,600 was seized from a suspect in April 2017 who was challenged as he drove into Gibraltar. He claimed that he was paid in cash from his employment as an underwater welder.

He was unable to provide documentary evidence in support. The Prosecution applied to extend the period of detention. The suspect's mother advanced in court that she had lent the money to her son and that the cash originated from her furniture business in Spain. She provided bank statements. The Court ordered a short extension to the detention period in order for officers to examine the new material and the suspect's mother consented to a civil interview. Eventually she admitted that the large cash payments into her bank had never been through the company's accounts and she was evading paying tax.

There was no evidence of tax evasion in Gibraltar from a business she had recently established and from which no tax return was yet due. The forfeiture application based on the cash being the proceeds of criminal conduct in Spain was unchallenged. The GFIU disseminated information to the Spanish, Dutch and US FIUs.

154. The assistance of the GFIU is valuable to LEAs in the development of evidence in an on-going investigation and in tracing the proceeds of the crime. Both the RGP and HMC provided to the assessment team numerous examples of information requests on specific subjects: in cases of fraud the request would typically be in respect of specific bank transfers and for information on fraudulent accounts; in cases of drug trafficking and tobacco smuggling, the enquiry might be for details in respect of whether the suspect had maintained a business relationship with specific companies, businesses or natural persons. See the case studies below.

BOX 2 – CASE STUDIES (Use of information provided by the GFIU in RGP and HMC investigations)

Case 1

HMC are investigating a ML case where an individual had been making high deposits into a couple of local FIs. The GFIU provided intelligence into deposits going back to 2009, whether third parties were holders of the accounts and the name of a staff member at one of the institutions who was tipping off the suspect about an investigation by the financial institution where this person worked. As a result of the intelligence provided by GFIU, HMC obtained a search warrant for the suspect's home address and although the search yielded negative results, they are still conducting enquiries.

Case 2

As a result of intelligence by HM Customs, a subject, suspected of supplying drugs, was searched and found to be in possession of a Class A drug. The subject was suspected of supplying drugs to others. HMC executed search warrants on two residential properties. The GFIU obtained from two local banks intelligence in respect of five years of transactions of the accounts. Based on their analysis of the cash deposits and on the evidence of predicate offending a ML investigation was commenced which is still on-going.

Case 3

The ECU requested the GFIU to carry out checks with all local FIs in respect of two Dutch Nationals and two companies. Four bank accounts were discovered in the name of the Dutch Nationals. The ECU'S investigation, in conjunction with foreign LEAs is on-going.

Case 4

HM Customs are currently investigating an alleged fraud and evasion of duty in which the subject was importing high value vehicles and producing false documents to significantly underestimate their value. In some cases the documents falsely represent the vehicles as hybrids which carry a 0% duty. HMC executed a search warrant on the premises and some bank documents were retrieved. GFIU obtained documents relating to opening of these accounts and the transactions within them; weekly transfers were being made to a bank account in Spain. The bank was contacted, and both the accounts put on a risk alert. When attempts were made to transfer funds the GFIU stopped the transactions taking place. The investigation is still active.

155. The table below sets out the data for ML and FT related investigations, prosecutions and convictions. One of the four ML related prosecutions and convictions achieved (also elaborated

under I07) in the reviewed period was triggered by an initial STRs/GFIU intelligence report (Operation Flame). No FT investigation resulted in a prosecution.

Table 12: ML and FT related investigations, prosecutions and convictions Period 2014-2018⁴⁹

	Investigated		Prosecuted		Convictions	
	Cases	Individuals	Cases	Individuals	Cases	Individuals
ML	49	75	7	10	4	4
FT	15	24	0	0	0	0

3.2.2. STRs received and requested by competent authorities

156. The GFIU acts as the central authority for the receipt of reports from REs and public authorities.

157. Each STR is analysed and subjected to a preliminary assessment. If the STR does not meet the required standards, additional information from the RE may be required (see also paragraph 134). STRs from specific sectors (e.g. from the gambling industry) are always shared with the supervisory authority and are of use in the identification of potential typologies specific to the sector.

158. The process of analysing STRs is achieved using 3 priority levels (low, medium and high). For high priority cases (FT), the analytical process is undertaken immediately, assessing the need for additional information from the RE, and whether the case may be disseminated that day to the LEA and kept under review after the submission is made.

159. The authorities advised that the period needed to analyse and further disseminate a STR ranges from one to several days. Themis has facilitated the process. STRs which do not result in a further intelligence report and are not therefore disseminated to LEAs, are stored in the GFIU database. These STRs may be further reviewed in the event that there may be other STRs which are related to them or that they may further serve in case related requests for information from Gibraltar's LEAs or foreign FIUs.

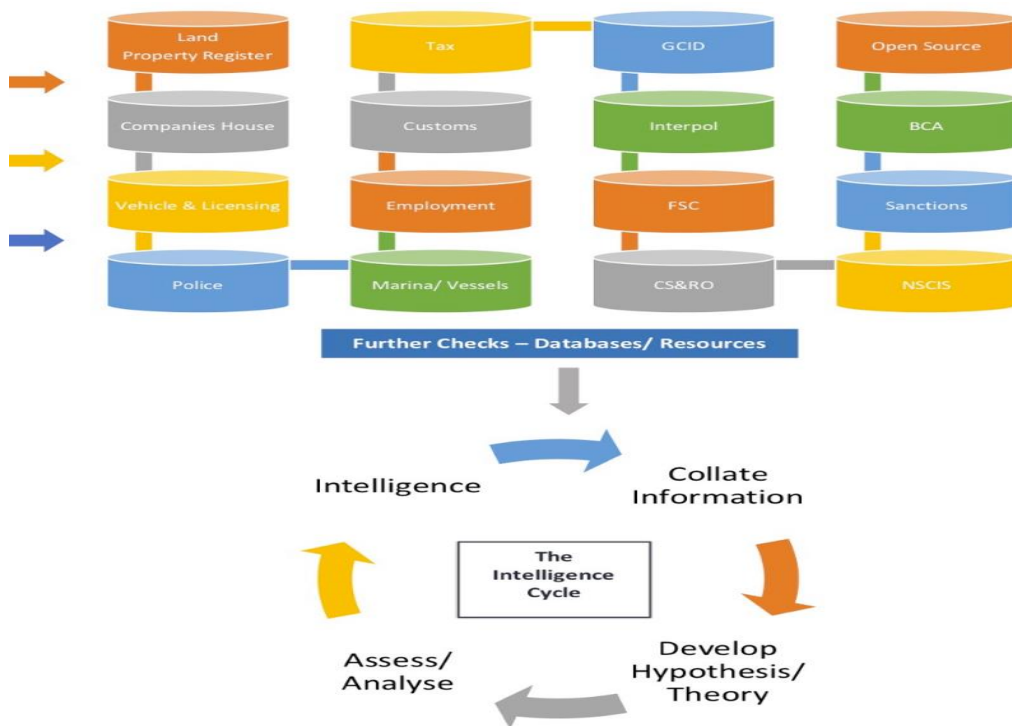
160. SARs submitted from the Gaming Companies which refer to UK nationals or UK companies are also sent to the UK FIU (NCA) through the Egmont Secure Web (ESW) because the GFIU may hold information of intelligence value to the UK FIU. All other SARs relating to foreign subjects or companies are sent to the relevant country through the ESW.

161. In cases where an STR does not indicate data on transactions which were carried out within the financial system of Gibraltar, spontaneous information is immediately sent to any counterpart FIU. Once a preliminary assessment of a STR's content is made, if any transactions are within Gibraltar alone, searches against any relevant person are conducted through the GFIU database and through other databases to which the GFIU has direct access or access upon request. The GFIU has adopted a policy document for quality assessment and control of STRs, setting out the steps to be taken in respect of quality assessment, co-operation with the supervisory authorities, feedback to the REs and the permanent monitoring of a STR's quality. Although some guidance is provided (e.g. the Protocol for requesting information to determine whether a person is a holder or BO of one or more accounts; protective marking as a security system for the creation, handling, storage and disposal of documents, data and information; different forms and workflow schemes) no proper operational manual for the analytical process has been developed, which

⁴⁹ In early 2019 another ML there was another prosecution and conviction but given the incomplete statistical data for 2019 the table only shows figures up to 31 December 2018.

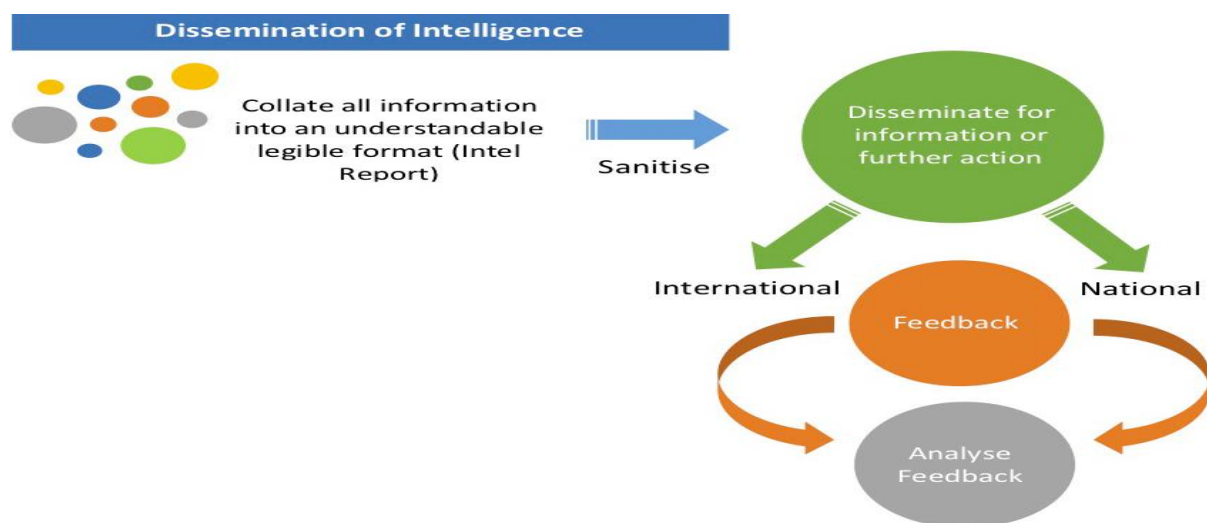
would assist GFIU analysts. The scheme presented below explains, in general, the process of checking different databases upon which the analysis is completed.

Table 13: Further Checks - Databases



162. To make an assessment of any grounds for suspicion of criminality in the intelligence report, it is first reviewed by the grading officer of the GFIU. The report is then sent to the operations manager for approval and then disseminated. As noted already, intelligence reports deriving from STRs from the sectors supervised by the GFSC and GGC are also sent to these authorities. If an STR includes data which is indicative of tax infringements, then the intelligence report is sent to ITO in addition to the LEAs.

Table 14: Dissemination of Intelligence



163. HMC sends information to the GFIU (in the form of spontaneous disclosure or as a request for additional information) on all cash seizures and any drug related offences they investigate. HMC would also provide information on any cross-border movement of currency to outside the EU. Whilst the system for declaration of cash has been in place since March 2018, no cases of

undeclared or falsely declared cash were detected in the reviewed period. The RGP sends spontaneous information to the GFIU in the following circumstances: whenever the RGP investigates ML or FT; where there may be no investigation of ML or FT but where dissemination might be beneficial: investigations into drugs and human trafficking were the subject of such disclosures. In the period 2017-2019, HMC sent 39 disclosures to the GFIU whilst RGP sent 16.

164. Concerns remain in respect of the quality of STR reporting in some important sectors. Given Gibraltar’s role as an international financial centre, there is a question as to whether sophisticated ML with predicates committed abroad is likely to be detected through suspicious transaction reporting. Only one case of ML leading to a conviction has been triggered so far by a STR and that was a case of domestic self-laundering ML (operation Flame). The assessment team can only conclude that STRs are either not being received which would enable the detection and investigation of sophisticated ML deriving from foreign predicates or, if received and put into disseminations to LEAs by the GFIU, those disseminations are not effectively leading to investigations and prosecutions resulting in convictions. The AT considers that although both scenarios may apply, the underlying problem is the scarcity of quality STR reporting. The GFIU has increased its outreach to REs in an effort to improve the quality of STRs. Guidance for MLROs and other reporters on the SAR regime was provided to all REs. This guidance includes both identifying ML and FT indicators and detailed instructions on how to produce better quality SARs. The guidance, however, does not include any typology or any sector specific approach. Feedback on the quality of STRs is regularly communicated to REs. Project Nexus was used as a platform for the discussion of issues such as public and private sector cooperation and for advice on good practice. Although it appears that the quality of STRs increased in some areas (e.g. the largest FIs), any overall benefit deriving from these initiatives is yet to be seen. FT suspicious transaction reporting was the subject of a specific GFSC analysis (AML/CFT (Conflict Zones) – An assessment of Exposure and Vulnerabilities). There is analysis of the data for overall transactions (incoming and outgoing) from and to high risk jurisdictions. For the banking sector, for example, in 2017 around 30,000 transactions were executed (incoming and outgoing). No FT STR was submitted by banks in that year. The GFSC noted that this fact could potentially raise some concerns and, at the very least, warranted further investigation as to why this was the case. By the time of the on-site visit such an investigation had still to be carried out by the GFSC. Additionally, the shortfall in the provision by the authorities of sector specific FT guidance to the various FIs and DNFBPs which is likely to have had a negative impact on the taking of effective action. The following table shows the total number of STRs received by the GFIU in period 2014-2018.

Table 15: Number of STRs

	2014	2015	2016	2017	2018
Number of STRs	532	618	91	1660	2892

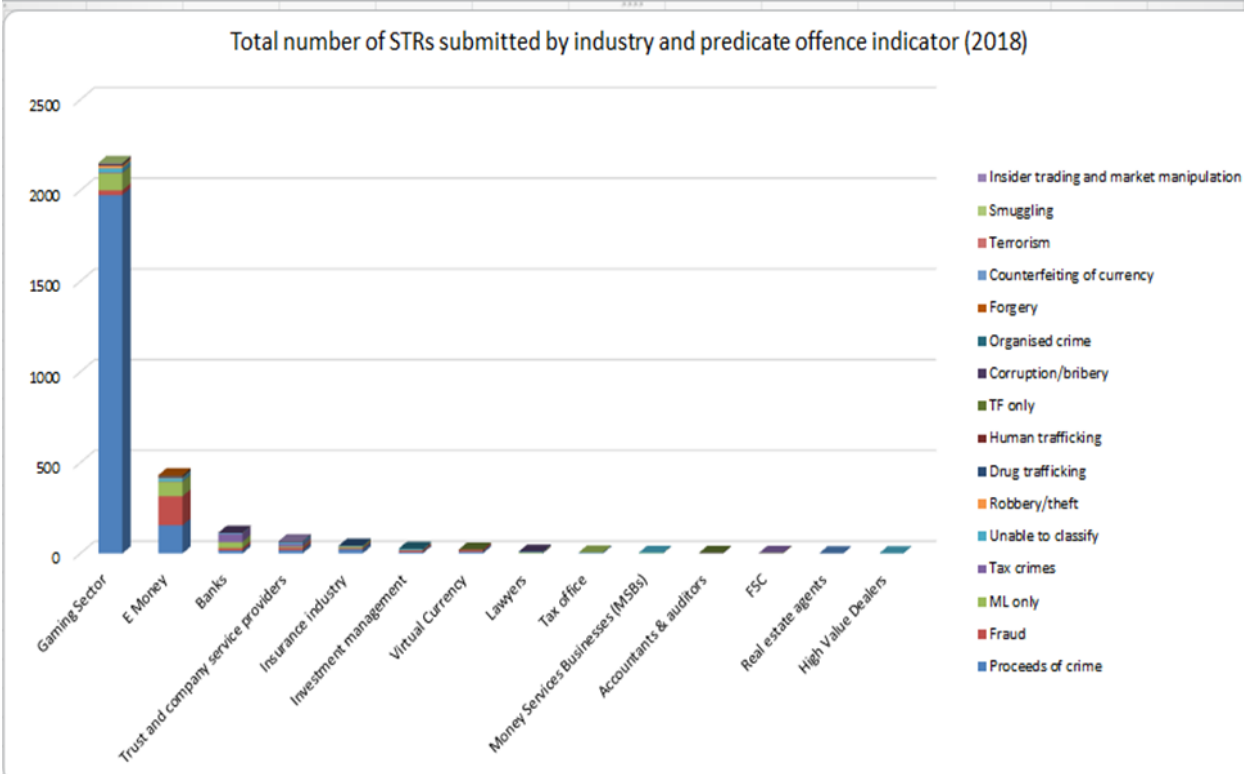
165. The increase has been substantial particularly from REs within the gambling industry. The gambling sector submits 73% of all STRs. According to the GFIU a typical example of an STR in this industry is concerned with an inability to reconcile a customer’s profile with the amount the customer is spending. The reason behind the rapid increase of STRs submitted is also attributed to the UK Gambling Commission fining one of the local gambling providers. This has resulted in over reporting by the industry, even in respect of past events. To address this issue, a GGC official has been seconded to the GFIU, ensuring that the Remote Gambling Industry applies a consistent approach to AML/CFT reporting. It is hoped that Project Nexus also raised awareness in this particular sector. Both the GFIU and the LEAs confirmed that the value of these STRs to investigations by LEAs was insignificant.

166. Banking sector STRs were usually but not exclusively linked with tax declarations. The subjects of these STRs resided outside Gibraltar but may have possessed assets in Gibraltar and/or abroad. A typical STR typology for the banking sector was for potential ML giving details of assets held and/ or transactions to and from the account(s) of a natural person who was the bank’s client (prompted usually by a match to open source information on that individual being accused or convicted of crime).

167. TCSP SARs were triggered by failures in the due diligence process, concerns about source of wealth and matches with different lists. A total of 240 STRs were submitted by the sector in the reviewed period. Overall, the assessment team is of the opinion that the reporting from banking and the TCSP sectors, given the risk and context of the jurisdiction, warrant further analysis by the competent authorities as to the reasons why the disseminations made were not leading to investigations followed by prosecutions (see also the potential underreporting by these entities noted under IO4).

168. Statistics on STRs submitted by different sectors of industry in 2018, with the types of predicate offences indicated is provided below. Statistics are also available for 2017 but the figures there do not differ much from those presented below. The overall number of STRs, submitted by the gaming sector and e-money is considerable. Reservations about the relevance of these STRs were elaborated above. The number of STRs submitted by other sectors, including banks, given the risks and context of the jurisdiction, appears to be rather low.

Table 16: Total number of STRs



169. As can be observed from the table above, the main predicate offence indicators in the STRs/disclosures received at the GFIU are Fraud, ML and Proceeds of Crime related offences. In 2018, 8% of STRs were related to fraud, 8% ML and 77% Proceeds of Crime - the latest being a result of the fact that the gambling industry do not have a defined predicate offence but they suspect that the customer is gambling with the ‘proceeds of crime’. Gambling with criminal property would, in fact, amount to ML.

170. The assessment team is of the opinion that the competent authorities do not receive reports which (to a satisfactory extent) contain relevant and accurate information to assist them in performing their duties. Although the GFIU respond to any information request from the competent authorities, the outcomes of these exchanges are yet to bring results along with the on-going investigations they were a part of. From the disclosures received neither the GFIU nor the LEAs have identified ML typologies which are typically encountered in Gibraltar and which would enable both the GFIU and the LEAs to streamline their efforts and better deploy available resources.

3.2.3. Operational needs supported by FIU analysis and dissemination

171. To some extent, the GFIU's financial analysis supports the operational needs of relevant LEAs to pursue the investigation of predicate offending, ML and FT. The LEAs acknowledge that the results achieved for the period under review were modest and further efforts (including prioritisation by them of cases triggered by GFIU intelligence) will be needed to foster an effective use of the GFIU's products. One of the indicators of the limited use of the GFIU analysis is the gap between the number of STRs received from the REs and the number of GFIU disseminations to LEAs (please also see Table 6.1). In the period 2014-2019 the GFIU received and analysed 6616 STRs and these gave rise to 269 disseminations to LEAs. 110 of these disseminations were also sent to the supervisors so that they could better inform their RBA in carrying out their controls.

Table 17: Number of disseminated reports per annum

	2014	2015	2016	2017	2018
RGP	73	43	52	44	25
HMC	2	7	4	9	2
GFSC⁵⁰	6	39	14	6	10
ITO	3	12	0	5	3

Table 18: Statistical data on STRs/disseminations for FT

	2014	2015	2016	2017	2018
No. of FT STRs received by the FIU	9	18	13	6	9
No. of FT STRs disseminated to / accessed by law enforcement agencies	5	1	4	4	2
	2014	2015	2016	2017	2018
Number of cases investigated for FT	5	1	3	3	3
Number of FT investigation initiated by STRs	5	1	2	3	3

172. The LEAs confirmed that the vast majority of STR analyses that they received from the GFIU were where an investigation had already been commenced by the RGP. Their understanding is that, once the RE became aware that an investigation had been initiated (through the media or any other source) then the RE immediately prepared a STR and sent it to the GFIU. In addition to this, the assessment team also noted that defensive reporting was typical for some sectors (gambling industry but also some FIs). Such reporting/STRs were of limited value for LEAs and the information held therein tended only to repeat what the LEAs had already obtained (through requests) in the course of the investigation. Typically, the analysis performed by the GFIU did not provide tangible support to the operational needs of the competent authorities. This appeared to be the major reason why STRs have generated very few investigations.

173. The GFIU disseminate SARs to the supervisory authorities such as the GFSC and the GGC, but also to the ITO when there is a suspicion that tax crime has been committed (please also see the cash seizure case study above). Discussions held on-site on cases presented by the authorities did not provide sufficient evidence of these GFIU reports making a tangible impact in tax related investigations or on the effectiveness of supervision (for the latter please read IO3).

174. The GFIU analysed all STRs received in any one year. There had been a dramatic increase in the number of STRs received in 2017-2018. Although the number of staff had been increased to meet the additional workload, the turnover in staff continued to be an issue. New staff also needed periods of training before being able to conduct analysis. Taking as an example, the year 2018, with 2892 STRs received, 4 full time analysts with 250 working days a year, would each have needed to analyse on average approximately 3 STRs a day. The fact that is necessary to make proper checks and take further steps for each STR puts in question the GFIU's capacity to properly analyse the STRs received. The GFIU team is composed of a total of 11 officers; 3 seconded from the RGP, 3 from HMC, 4 permanent civil servants (3 transferred from the GFSC, and an administration officer), and 1 embedded from the Government's Gambling Division on a part-time basis dealing with analysis of Gambling related SARs. Overall, six of them are dedicated to the operational analysis of SARs.

175. For the GFIU staff there was an introductory course and later NCA training on financial intelligence. The financial intelligence officers' backgrounds were the RGP or HMC. The CFT expert had an intelligence background.

176. The continuous turnover of seconded staff is considered to be an issue that affects the operational capabilities and expertise of the GFIU. There is an urgent need to ensure staff retention and it would be advisable to opt for permanent rather than seconded staff for the GFIU, particularly where those staff are engaged in analysis. There is no operational manual in place, which would help with the on-boarding process of new employees.

177. Strategic analysis is an area where further efforts need to be invested and this has also been noted by the GFIU. The strategic analysis training undertaken by the GFIU's staff is considered to be insufficient. So far, the GFIU has produced one strategic analysis - "*An analysis of the Suspicious Transactions Reporting in Gibraltar for 2018*". The analysis focuses on the two largest reporting sectors of 2018 (gaming sector and E-money), which produce approximately 80% of the total number of STRs. The topics covered were as follows: quality issues with the STRs; gambling trends; the proper identification of clients; concerns relating to false documents. The analysis also provided mitigating measures. No specific typologies have been produced to date. More efforts need to be invested by the GFIU in the following areas: the training of its analysts (this is especially important); defining the typologies typically encountered in Gibraltar and those which one would expect to see encountered in Gibraltar given it is an international financial centre; the identification of typologies would assist the GFIU's analysts in providing intelligence in respect of complex ML schemes that may be occurring in Gibraltar.

178. The analysis has not yet been disseminated to the private sector or supervisors.

179. The GFIU does not use specific software designed for the FIU analysts and currently uses IBM's i2 software for these purposes but is in the process of purchasing specialist forensic software which will also enable data interconnection with databases, financial analysis, and intelligence reporting.

180. The Themis database, designed mainly for reporting and exchanging information in electronic form, allows for database searches and the integration of requests in electronic or manual format. As already noted, prior to Themis, the GFIU received SARs in hard copy form which were then integrated in the IBM iBase i2 Analyst's Notebook, which is used by both the GFIU and

the RGP, enables the development of multidimensional visual analysis (e.g. recording/monitoring complex financial data, visualisation of connected networks, links among persons involved, aggregated data, etc.).

181. The assessment team have no reason to question the operational independence of the GFIU. There is no evidence to indicate that the GFIU's analysis and dissemination functions have ever come under any political, government or industry pressure.

3.2.4. Cooperation and exchange of information/financial intelligence

182. Inter-agency cooperation in Gibraltar is good. The GFIU is in permanent contact with the competent authorities, both LEAs and supervisors. The fact that RGP and HMC have their staff seconded to the GFIU further fosters cooperation between these institutions and facilitates a prompt response to different requests. The LEAs always inform the GFIU about and, where necessary also engage the GFIU to provide further intelligence, in their investigations. A range of MoUs on information exchange were signed, involving all competent authorities. The aim is to foster further interagency information exchange and cooperation. In February 2019 the RGP, HMC, the GFSC and the Tax Office signed a MoU ('Agreement on Joint Task Force for Operation Fusion.') All the signatories committed to disseminate appropriate intelligence to each other, ensuring the protection and confidentiality of data. There are no impediments to the exchange of information.

183. The GFIU co-operates well with foreign FIUs. The introduction of the POCA (in 2016) fostered further the ability of the GFIU to obtain additional information from REs. Case studies are provided below.

BOX 3 – CASE STUDIES

Case 1

Late on Friday 18th November 2016 the GFIU received a call from France FIU. The nature of the call was that the French authorities were trying to prevent an imminent terrorist plot and it was extra urgent. A DPA request for information was immediately sent to a local pre-paid card company. The company replied promptly stating that the information required was with another company. The GFIU contacted France FIU and was able to point them in the right direction. The French FIU informed the GFIU that they had also approached the NCA regarding the case. The GFIU was able to rule out the local company as the source of the information and point France in the right direction. The French sent the GFIU the official request through Egmont the following Monday. Over the course of that weekend 3 French persons were arrested for terrorist related offences.

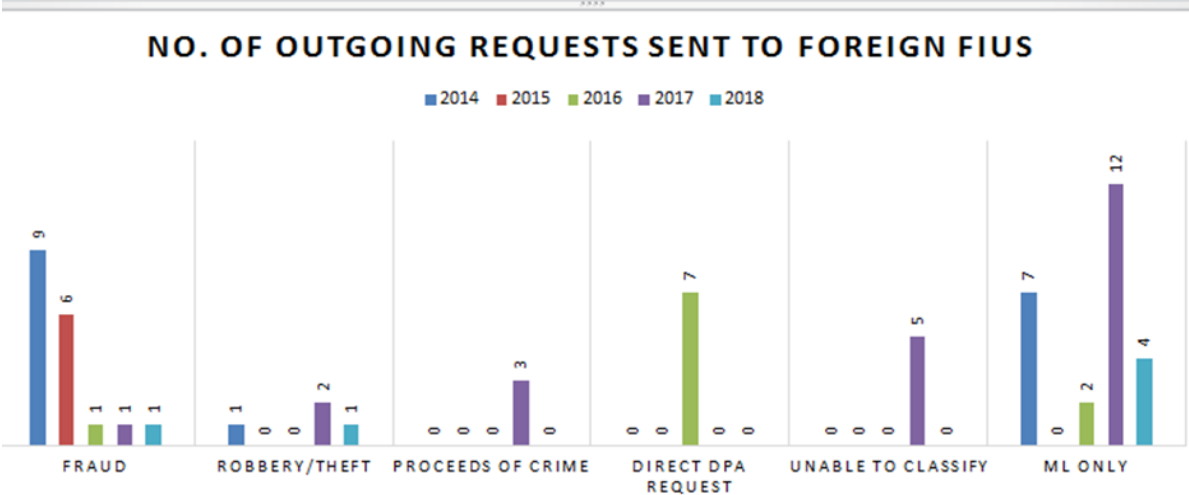
Case 2

On the 23rd November 2016 the GFIU received a letter of request from the Isle of Man asking for assistance with a case concerning theft of cash from an employer. The subject was a compulsive gambler and it was believed that some of the funds in question had been used to support his gambling habit with a Gibraltar based gambling company. The subject fled the Isle of Man to the UK. He was apprehended by UK authorities where he eventually pled guilty to two charges of theft from his employer. The GFIU retrieved the relevant intelligence from the local gambling company and forwarded it via Egmont to the Isle of Man on 01/12/2016. In 2019 the GFIU learnt that the subject had been sentenced to eight months imprisonment for each of the two thefts.

184. The table below sets out the number of requests the GFIU sent to their foreign counterparts for each broad category of crime. The figures are low, relative to the risks and context of Gibraltar as an international financial centre. Although exact figures are not available to establish the extent to which the information received from abroad was further used to develop evidence, trace assets or initiate investigations into ML/FT or associated predicate offences, the interviews held on-site

suggest that this was rarely the case. The GFIU received a significant number of requests from foreign FIUs. Around 240 of these requests were related to ML and very few to FT. Whilst the GFIU responded diligently to most of these requests the material in these requests and the information solicited following their execution were not further examined/used to detect eventual involvement of Gibraltar entities or person in ML/FT schemes. The authorities argued that the reason these requests did not end up in local investigations is because these requests related mostly to online gambling and e-money whose subjects were out of the jurisdiction and already investigated for ML by the originating country. Whilst the assessment teams acknowledges this argument, it still considers that information/requests received from the foreign jurisdictions warrant further analysis to determine whether or not the proceeds of offences committed abroad were laundered in Gibraltar or if any of the laundering phases abused the jurisdiction’s financial services or products. The RGP also seeks intelligence from abroad to investigate ML/FT and predicate offending. The RGP presented to the assessment team a few examples where they proactively sought assistance from abroad; none of these cases have yet resulted in a prosecution. A decreasing trend in the number of requests made by the RGP was observed in the review period. The RGP explained that this decline in outgoing requests was caused by (i) the employment of substantial human resources on significant/big cases and (ii) the fact that there were a number of informal requests which did not form part of the figures as a result of the developed face to face cooperation with some of their foreign counterparts.

185. **Table 19:** FIU to FIU outgoing Requests



186. The GFIU uses to send a relatively high number of spontaneous disseminations to foreign FIUs (detailed statistics are included under IO2). From 2017 the criteria for selecting cases upon which requests to foreign FIUs were made and those in which spontaneous disseminations were sent have been changed: the GFIU does not disseminate to foreign FIUs STRs already disseminated by the gambling industry to UK FIU. If there are no further data held at the GFIU on that particular STR, no further dissemination is made to foreign counterparts. This has significantly decreased the number of outgoing requests or spontaneous disseminations.

187. The GFIU staff is locally vetted and have signed the UK Official Secrets Act 1939. Furthermore, RGP officers seconded to the GFIU are vetted by the UK Security Vetting Agency to SC(E) and DV level.

188. The GFIU has a Protective Marking Scheme Policy which protects documents and provides advice on handling, storage and access. Furthermore, the GFIU applies HMGoG’s security policy on IT. S11C of POCA governs the exchange of information and the dissemination of GFIU information to other FIUs and domestic competent authorities.

189. The IT system of the GFIU is maintained by the HMGoG ITLD and all data is stored securely in government servers. The GFIU applies HMGoG Policy on IT Security. The new STR online reporting program (though Themis) requires a Partnership Agreement for End Users (LEAs) to be signed and sets out the requirements, responsibilities and implications for access. The system provides an auditable trail of any searches conducted and any breaches of the agreement will be reported, and access may be withdrawn by the Head of the GFIU.

190. The ESW is the only system that is used by the GFIU to transmit financial intelligence or information to foreign FIUs that are members of Egmont. The transmission of data between LEAs and the GFIU is done via the HMGoG internal email system. There are instances where international informal channels are used to exchange information, but these are always followed by formal channels using ESW.

Overall conclusions on IO.6

191. **Gibraltar is rated as having a low level of effectiveness for IO.6.**

3.3. Immediate Outcome 7 (ML investigation and prosecution)

3.3.1. ML identification and investigation

192. From May 2016 the Money Laundering Investigation Unit (MLIU) was created within the RGP in response to a growing awareness of the threat of ML and FT and the fact that that threat was not being effectively addressed.

193. The 2017 HMGoG AML/CFT Strategy at section 3 identifies that “Despite the best efforts of stakeholder authorities to prevent ML/FT from occurring in the first place there will be those persons who through inaction or wilful participation will either launder proceeds (self-launder or third-party laundering) or not put into place adequate systems of control to prevent their business from being used for ML, FT or PF.”

194. Gibraltar’s Policing Plan 2018-2019 under the heading “Tackling Crime Proactively and Effectively” at point 10 of the delivery plan has “The RGP will increase detections of ML offences.” Although the detection of ML might be identified as a priority issue, no specific strategy is set out in any of the authorities’ documentation in respect of the need to effectively investigate and (as far as the Prosecuting Authority is concerned) effectively prosecute ML, nor is the programme set out by which these twin functions may be achieved.

195. The RGP and HMC are the two LEAs in charge of ML investigations. The RGP created the MLIU in May 2016 in response to this understanding of the AML/CFT risks posed to Gibraltar. The RGP maintains an Economic Crime Unit (ECU) under which sits two departments, the MLIU and the Fraud Squad. The MLIU of the RGP is made up of one Inspector (in charge of both the MLIU and Fraud Squad), one Sergeant and 3 Constables. The Fraud Squad has one Sergeant, 3 Constables and 3 part time civilians who are retired experienced former Police Officers. HMC may initiate ML investigations when i) investigating predicate offences for HMC assigned matters; ii) receiving SARs from the GFIU; iii) receiving intelligence reports from within HMC or from third parties; iv) carrying out cash seizures; and v) checking cash declarations.

196. So far all ML investigations were initiated by the RGP.

197. There seems to be no impediment to inter-agency cooperation and coordination of ML investigations and prosecutions, including the timely access to relevant financial intelligence and other information needed to build a case. Joint and co-operative investigations and information exchange between different competent authorities such as the RGP, HMC, the GFIU and the GFSC are possible and have occurred (please see case ‘Exodus’ below).

198. Given the fact that Gibraltar is an international financial centre, even when one takes the size of the jurisdiction into account, the number of ML cases investigated is low and the number of ML investigations leading to ML prosecutions is extremely low.

Table 20: Number of ML Investigations, Prosecutions & Convictions with or without a STR/ SAR

Year	ML Investigations whether leading to a ML Prosecution or not		ML Investigations NOT leading to ML Prosecutions		ML Investigations leading to ML Prosecutions		ML Prosecutions Resulting in a ML Conviction	
	Cases	Persons	Cases	Persons	Cases	Persons	Cases	Persons
2014	0	0	0	0	0	0	0	0
2015	0	0	0	0	0	0	0	0
2016	20	30	20	30	4	7	0	0
2017	8	15	8	15	1	1	0	0
2018	21	30	19	28	2	2	4	4

199. It will be seen from the figures above that in 2014 and 2015 there were no ML investigations conducted at all. In 2016, there were 20 ML investigations commenced, four led to a ML prosecution; there were no convictions for ML in 2016 or 2017. In 2018, there were 21 ML investigations, 2 ML prosecutions and 4 ML convictions arising from prosecutions commenced in that year or preceding years. There were therefore 4 ML convictions in total over the reviewed period. All 4 were guilty pleas. All 4 were self-laundering cases. There have been no third party ML prosecutions leading to a conviction in the period under review. One of these convictions was for a standalone ML prosecution - a convicted street dealer of drugs who was self-laundering (Operation Doorstop). The Defendant's transactions through his bank account could not be accounted for by him from legitimate income. Evidence of his drug dealing was not relied upon in the ML Prosecution. By his plea of guilty to ML he accepted that the funds concerned were criminal property. The other standalone prosecution in which the Prosecution are not adducing evidence of the predicate criminality concerns a male street dealer of drugs (the self-launderer) and a female who is alleged to have acted as a 3rd party launderer in assisting him (Operation Gulf). The case has commenced in the review period has not yet been tried and is on-going.

200. ML investigations, in almost all cases in Gibraltar are initiated by an investigation into the predicate offence. The reason that so many ML investigations do not lead to a ML prosecution in the last 3 years covered may be manifold. The focus may have been on the predicate offence not on any ML offence and the aim of financial investigations would have been limited to obtaining evidence that would support the prosecution of the predicate crime and identifying assets which might be confiscated in the event of a conviction for the predicate crime. Given the fact that Gibraltar is a financial centre, the focus should have been on the laundering of funds originating from predicates committed abroad and their integration through the Gibraltar financial system using products and services offered by the jurisdiction. Over the review period there have been two such investigations but those have not yet reached the charging stage. The RGP acknowledges the need to address this typology but advanced that it has limited resources and must continue to tackle OCGs laundering in Gibraltar the proceeds of drugs trafficking from outside the jurisdiction. The RGP suggested that there is a balance between tackling all forms of crime in Gibraltar and the laundering of foreign predicates through Gibraltar as a finance centre. ML investigations into third party ML leading to standalone ML prosecutions do not appear to have been a key objective for the LEAs and prosecuting authority in the past. There is evidence that this is changing; there are currently at least two significant investigations into the 3rd party laundering of foreign predicates. These may give rise to stand-alone ML prosecutions. The RGP comment that these are taking up most of the MLIU resources.

201. The great majority of cases which were investigated did not lead to a ML Prosecution. As already discussed under IO6, the RGP explained that this may have been due to a variety of factors such as: i) the investigation may have amounted to no more than the necessary checking of whether a low-level drugs suspect had assets and if he did not, then there would be little merit to pursuing the matter any further; ii) the defendant admitted the predicate offences, those offences would attract a high sentence and no ML charge was thought necessary; iii) lack of resources - it was necessary to focus limited police resources on more serious ML investigations (most of these have not yet concluded and were not incorporated into the figures above). The assessors were impressed by the commitment of the members of the MLIU and their desire and ambition to be more effective in this area.

202. By far the largest number of ML investigations (28 in all over 3 years) was linked to drug trafficking and because the defendants may have been low-level user/ dealers they may not have been prosecuted for ML because no criminal property was located for them to have laundered. Financial crimes investigated were also typically domestic and tended to involve a Gibraltar resident stealing from an employer.

BOX 4 - Case Study (ML conviction)

The Defendant entered guilty pleas on two indictments to counts of possession with intent to supply cocaine weighing approximately 15 grams. The cocaine had a purity of 81%.

Prior to his guilty plea to the drugs offences, following an investigation into his finances, it was discovered that between 1 January 2015 and 28 February 2015 the Defendant paid into his bank account cash totalling GBP 17,535. The cash paid into his bank account was the proceeds of criminal conduct. The defendant was charged with ML to which he pleaded guilty. He was sentenced to 16 weeks imprisonment for ML consecutive to his custodial sentence of 5 years and 9 months for the drugs offences.

An application was made for a confiscation order. The Defendant had assets in the Gibraltar savings Bank.

As the defendant contested confiscation the matter was adjourned for 6 months pursuant to sections 35 and 36 of POCA to enable the RGP to conduct a confiscation investigation.

203. The figures would appear to suggest that the authorities have not in the past proactively identified and prioritised the detection, investigation and prosecution of complex ML cases in which elements of Gibraltar's financial centre have been potentially abused to launder the proceeds of foreign predicates. Although the RGP's flow chart entitled "ML investigation take on criteria" (RGP 15, which appears to be dated June 2018) makes reference to "NRA Correlation," being a factor to be considered when deciding whether there should be a ML investigation, it does not prioritise the investigation and prosecution of the ML of foreign predicates per se nor does it emphasise the need to conduct a parallel ML investigation in all cases involving (major) proceeds generating crime - particularly where Gibraltar's financial sector may have been misused to launder criminal property. This would also apply if the investigators were of the view that it could be established that the property laundered was criminal property even in circumstances where the type of predicate crime was unknown.

204. The statistics in the Table 16 above may provide too small a sample to enable firm conclusions to be reached about the quality of SARs/intelligence reports received from the GFIU and their lack of impact in creating an effective AML regime. More about the use of financial intelligence is provided under IO6. Nevertheless, only one of the four ML cases in which there was a prosecution leading to a conviction was initiated by a SAR. The case is presented in the box below.

BOX 5 – Case study (Operation Flame)

The Defendant entered a guilty plea to one count of false accounting and one count of ML. Essentially the Defendant used fraudulent documentation including pay slips, which showed that he was employed at his sister's tobacco shop, to open an account with a local bank, into which he made cash payments on diverse occasions amounting to GBP 15,000 the monies being the proceeds of criminal conduct, believed to be unlawful tobacco activity. The conversion of criminal property into what were disguised as lawful cash deposits was the first stage of the ML process. The Defendant was sentenced to a high-level Community Order requiring the Defendant to undertake 240 hours of unpaid work.

The court also made a confiscation order pursuant to section 35 and 36 of POCA whereby the Defendant agreed that he has benefitted from his particular criminal conduct in the sum of GBP 46,928.59. He was ordered to pay GBP 39,428.59 (this being the realisable amount).

205. No ML investigation seems to have been prompted by an incoming MLA request in respect of ML or a predicate crime committed abroad. The authorities advance the following points: since approximately 2017 incoming requests have been reviewed by the Inspector of the ECU as to whether there is any potential for a local investigation; the reasons for not starting a local investigation have been recorded since the start of 2019; outgoing material is supplied to the GFIIU for intelligence screening. That said, neither the incoming MLA requests nor, more importantly, the product obtained in satisfaction of those requests has given rise to an investigation as to whether persons within the financial sector in Gibraltar might be engaged as intermediaries in the laundering of the proceeds of foreign predicate crime and investigated and prosecuted within Gibraltar for such ML.

206. There is no forensic accountant within the unit. It is the responsibility of the RGP to decide which offences are charged. They may seek and be guided by advice from the OCP&L but the decision is theirs and a prosecutor may advise upon but not lead an investigation. So far as the Prosecution is concerned, one Crown Counsel is effectively allocated (in part) to financial crime. The assessors were informed a serious ML case would be conducted by the Director of Prosecutions – a role that was created in January 2019. The assessment team makes it clear that it is no criticism of the professionalism, ability or commitment of those in the RGP who investigate ML or those in the OCP&L who currently prosecute it, in observing that the effectiveness of the investigation and prosecution of ML in Gibraltar could not be said to be adequately evidenced by 4 convictions over a 5 year period. There may be a number of reasons for this and it may be the case that investigative opportunities were missed because of a lack of experienced prosecutorial input and/or focus in the past.

207. The assessors take the view that both the MLIU and OCP&L are not sufficiently resourced to deal with the investigation and prosecution ML cases of any significant scale which would be likely to be generated if the AML system was operating effectively. The OCP&L advanced that such cases would be likely to be resourced by instructing external counsel from England and Wales who would be admitted to the Gibraltar Bar specifically for the case in which they were instructed. Although the authorities observe that regular meetings are held between the MLIU and the OCP&L, the authorities might consider whether the AML regime would benefit from an experienced Prosecutor being embedded in the MLIU to advise on AML and financial crime. The Police and Prosecuting Authority differed on whether it would be more practical to draw upon the resources of an in-house forensic accountant or to instruct outside forensic accountants on a case by case basis. Whichever method is adopted many investigations cannot be scoped or advanced without early and thereafter continued support from a forensic accountant. If there is not adequate forensic accountancy input, there is a risk that the most serious ML investigations are either not commenced or are concluded prematurely because they were considered to be too complex.

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

208. The types of ML being investigated and prosecuted in Gibraltar are not consistent with the jurisdiction's threats, risk profile and AML policies. The four ML prosecutions and convictions over the review period arose from domestic predicate offending. The 2018 National Risk Assessment at paragraph 4.2 makes this observation about what might be learnt from the International Information Sharing Data: "In analysing what predicate offences would lead to the materialisation that an unmitigated risk exists, it is useful to look at data regarding international requests for assistance as Gibraltar's position as a provider of financial services to the international community would indicate that there are predicate offences committed elsewhere which would use Gibraltar based products and services to layer or integrate proceeds of crime."

209. The NRA shows that fraud, ML, drug trafficking and tax crimes predominate in the foreign predicates giving rise to these incoming international requests. Over the period under review, the investigative focus has not been aligned with the findings of the NRAs: there have been no ML prosecutions and convictions (either domestically initiated independently in Gibraltar or prompted as a result of an earlier investigation in a foreign jurisdiction) in respect of the ML in Gibraltar of the proceeds of foreign predicates. In the period under review, none of these international requests triggered domestic investigations into possible ML offences by REs such as TCSPs who may have acted as professional intermediaries and concealed or made arrangements in respect of criminal property or failed to report their knowledge or suspicion of ML. The LEAs have not in the period under review conducted successful investigations of complex and high-profile ML cases.

210. Another topic that assessors considered was whether the evasion of tobacco duty in Spain would be a predicate offence in Gibraltar. The question arises as to whether, when cash is brought into Gibraltar by Spanish nationals deriving from the earlier evasion of Spanish duty on tobacco (and for the purpose of further purchasing tobacco in Gibraltar for sale in Spain evading the Spanish duty on tobacco) a) that cash is criminal property which b) is being laundered in Gibraltar and c) would give rise to a ML offence justiciable in Gibraltar. The authorities in Gibraltar take this approach: the current law in Spain stipulates that only cases of tobacco smuggling, in which the value of the goods (tobacco) exceeds EUR15,000, can be dealt with as a criminal matter (unless there are additional offences such as resisting arrest or forming part of an organised crime group). Any amount lower than that will receive an administrative sanction. The quantity of tobacco ordinarily carried by any one individual is therefore well below this threshold, even if loaded into a car or small vessel. If caught, the person is likely to cut their losses (i.e. accept the fine and have the vehicle/vessel confiscated) and not resist arrest. Additionally, association with other persons will be very hard to prove in the majority of cases. Because of the nature of this low-level criminality, which in large part involves Spanish Nationals, there are no assets in Gibraltar liable to be seized other than cash detected at Gibraltar's borders, which will be dealt with by HMC using the cash seizure powers under POCA.

3.3.3. Types of ML cases pursued

211. The Prosecution has not been able to demonstrate an effective ability to prosecute a wide variety of ML cases. All 4 prosecutions were guilty pleas. All 4 were for self-laundering. In the reviewed period there has not been a convictions for 3rd party ML. Theoretically there ought to be no impediment to a stand-alone (or autonomous) ML prosecution: the absence of evidence of a conviction for the predicate crime need not be an impediment to a conviction in an autonomous prosecution if there is sufficient compelling evidence to infer the necessary elements of the ML offence from the surrounding facts and circumstances found. The authorities have not

demonstrated that they can effectively prosecute in 3rd party and autonomous ML cases. Only natural persons have been prosecuted and convicted for ML to date. Although catered for in the legislation, no cases of criminal liability of legal entities were brought before the courts. The awareness of LEAs on this particular matter and the possibility to further investigate corporate liability (including also for ML) is low.

212. The judiciary of Gibraltar is entirely independent and has an excellent reputation. The lower courts are presided over by the Stipendiary Magistrate. Jury trials would generally be before the Chief Justice of the Supreme Court. If there were a long running fraud or ML case to be tried before a jury and which would take up weeks or months of judicial time, the likelihood is that a very experienced Judge with specialised experience in dealing with financial crime would be brought in because the Chief Justice would need to continue to be able to service his wide range of Supreme Court work. There is a visiting Court of Appeal made up of High Court Judges from England and Wales. Appeals to the decisions made by the Court of Appeal are heard before the Judicial Committee of the Privy Council which is the court of final appeal for the British Overseas Territories.

213. The judiciary met on-site confirmed that there are no legislative barriers to successful autonomous or stand-alone ML prosecutions and convictions for the reasons set out under Recommendation 3 at criteria 3.5 and 3.8. In determining the appropriate sentence, the judiciary indicated that (as in England and Wales) they followed the sentencing guidelines issued by the Sentencing Council for England and Wales and judicial precedent from decisions of the Court of Appeal and the Supreme Court in England and Wales.

BOX 6 – CASE STUDY (3rd party ML investigation ('Exodus'))

Operation Exodus was concerned with a Trust and Corporate Service Provider licenced by the Gibraltar Financial Services Commission. An employee at the TCSP (together with his wife who was not an employee of the TCSP) was operating independently (and therefore without a licence) in providing company directors, company secretaries and nominee shareholders to companies incorporated in Gibraltar, the UK and the Seychelles. When the TCSP discovered the employee's activities, it reported the matter to the authorities. An investigation was commenced with three main strands:

- a ML investigation into the third-party ML by the Suspects, who formed and managed these companies, to launder criminal property generated by others;
- the failure to conduct adequate due diligence and keep proper records;
- conducting licensable activity without a licence.

The RGP and GFSC commenced a joint investigation with an officer of the GFSC working within the RGP offices. The GFSC's expertise in this area assisted in the effective investigation of this matter. Enquiries through Companies House revealed thirty Gibraltar companies, registered over an 11-year period (and the majority of which were registered to the defendants' address) had directors, shareholders and company secretaries who were not residents of Gibraltar. Open source checks revealed that some were PEPs, there were connections to criminal activity and one individual had possible links to a terrorist organisation. Intelligence disseminations and requests were made to numerous jurisdictions, but no MLA requests were ultimately sent. The employee and his wife pleaded guilty to unlicensed activity and the CDD and records offences but not guilty to the ML charges of making arrangements to launder criminal property. Those ML charges were ultimately discontinued, ostensibly because of lack of evidence. It is now accepted by the Prosecuting Authority that more might have been done and those charges might have been pursued to conviction.

214. The authorities have said that there are a number of more serious and complex ML investigations which are on-going, and the investigation and prosecution of ML is now afforded a

greater priority and pursued with greater understanding than it was in the past. There is currently, for example, an investigation into the trade-based ML of EUR 2 million of criminal property deriving from organised crime. Evaluators were shown the results of this investigation in which powers under POCA and CPEA were effectively used. This has occupied four officers of the MLIU for 8 months who have been assisted by a forensic accountant. Due to the fact that the investigation is still on-going, no further details will be provided in this report.

3.3.4. Effectiveness, proportionality and dissuasiveness of sanctions

215. The sentences for self-laundering in Gibraltar have attracted concurrent rather than consecutive sentences. Although case law is lacking in Gibraltar on sentences in ML cases, Gibraltar's judiciary indicated that they would always be likely to apply the sentencing guidelines issued by the Sentencing Council for England and Wales which are well defined, and which have been applied consistently in many cases. There is no reason to think that those guidelines when applied in Gibraltar as they are in England and Wales would be anything other than broadly effective, proportionate and dissuasive. The judiciary also confirmed that although they are greatly assisted by the guidelines, they were entitled to depart from them and might, for example, impose higher sentences than those envisaged by the guidelines where the offending might have tendency to undermine confidence in Gibraltar as a financial centre.

3.3.5. Use of alternative measures

216. No civil recovery applications, for which there is legislation, other than cash seizures had been brought by the time of the on-site visit. The authorities might well use the civil recovery process more frequently where there is insufficient evidence to obtain a criminal conviction. Cash seizures are frequently made by Customs when suspected criminal property in the form of cash is carried across the land border with Spain.

Overall conclusions on IO.7

217. **Gibraltar is rated as having a low level of effectiveness for IO.7.**

3.4. Immediate Outcome 8 (Confiscation)

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

218. The confiscation of the proceeds of crime, instrumentalities and property of equivalent value has been declared as a policy objective of all LEAs in Gibraltar. A number of strategic documents place financial investigations and the confiscation of proceeds of crime as a priority.

219. The 2017 HMGoG AML/CFT Strategy, at section 3.2 specifically states that as a matter of HMGoG policy, LEA and OCP&L will seek to determine any assets held or controlled by those perpetrating a predicate offence with a view to freezing, seizing and forfeiting these so that criminals may not benefit from their criminal activity. Similar steps will also be undertaken in relation to any assets which may have been used to commit the criminal conduct itself. Both criminal as well as civil powers will be used for these purposes. LEA and OCP&L will also pursue "lifestyle" confiscations where an individual life beyond their means.

220. This policy statement derives from numerous reforms that were taking place in the jurisdiction. A key piece of legislation (POCA) includes three different methods: (conviction-based confiscation, administrative ('cash detention') and civil recovery). Specialised units for asset tracing and the management of those assets were established and training for financial investigators was held.

221. The RGP set up the Money Laundering Investigation Unit (MLIU) in May 2016 to act as a specialised unit in order to conduct ML investigations and parallel financial investigations for major proceeds generating offences with a view to confiscating the proceeds and instrumentalities. The RGP takes the view that the identification of assets is an integral part of any investigation the ECU carries out into any proceeds generating offence. The RGP has defined their Standard Operating Procedure for ML investigations in the form of a chart which provides precise procedures and actions to be undertaken when such cases are investigated. There is also an assets identification checklist (elaborated further under par. 236) which is used to define lines of enquiry.

222. A system has been established through the publication of internal RGP orders (known as Force Orders), which are published weekly, whereby any officer can request a parallel financial investigation for any proceeds generating predicate offence. HMC carries out parallel financial investigations for (i) all customs cases which are being prosecuted, (ii) whenever an intelligence report is received (whether financially related or otherwise) and (iii) when cash seizures are initiated. The authorities further advised that, even though criteria which needed to be met for launching a parallel financial investigation were set, officers were encouraged to consider the situations outside of these criteria upon examining the essential facts (i.e. merits) of the case. A Standard Operating Procedure for Requesting a Parallel Financial Investigation for major proceeds generating crimes has therefore been developed (for officers from outside the MLIU). Given the jurisdiction's risk profile (including the threats posed by tobacco smuggling and drug trafficking) this appears to be a valuable tool for pursuing the proceeds of domestic predicates and thus increasing the effectiveness of the overall confiscation regime. This notwithstanding, LEAs regularly initiate parallel financial investigations for criminal offences committed in Gibraltar or for the crimes that take place at the border crossing points, whilst the same conclusion cannot be reached for cases involving funds originating from predicates committed abroad where there is integration or attempted integration through the Gibraltar financial system.

223. The HMC is the principal law enforcement agency responsible for the enforcing the regulations relating to the licensing, sale, storage and transportation of tobacco. The Tobacco Act 1997 empowers the HMC to forfeit tobacco and the instrumentalities used in the smuggling of tobacco (see paragraph 210).

224. The POCA empowers the RGP and HMC to search premises, vehicles and persons and seize cash. Where there may be insufficient evidence to charge but there are reasonable grounds to suspect that the cash is either the proceeds of unlawful conduct or to be used in unlawful conduct, POCA makes provisions for a detained cash investigation to be undertaken. The cash is recoverable if over the sum of GBP 1,000. The detention of the cash may be challenged in court. In the absence of any successful challenge, the seized cash is then retained (see also R.31).

225. The investigative responsibility for civil recovery lies with the LEAs, any application before the court is made by the OCP&L.

226. Notwithstanding the reforms undertaken, the results achieved during the period under review for the confiscation of the proceeds of crime, (or property of equivalent value) and the forfeiture of the instrumentalities of crime, are low. The very few cases in which confiscation orders were made involve domestic predicates (e.g. drugs, tobacco smuggling). This is suggestive of where the focus of the authorities has been directed. Taking into account the low figures for confiscation, especially when compared with the assets held and managed in Gibraltar and its role as a financial centre, it can be concluded that, although confiscation is stated to be a policy objective by the LEAs that stated objective has not been put effectively into practice. The low levels of confiscation do not accurately reflect the risks in Gibraltar.

227. The assessment team’s reservations with regard to the effectiveness of the confiscation regime are also revealed by the lack of usage of all of the range of available criminal, administrative and civil tools at the disposal of the authorities. For example, although a sound civil recovery regime exists since January 2016, it has not been used in practice. So far, no civil recovery case has been brought. Better results were achieved with (administrative) cash detention – this measure was applied in 35 cases resulting in the retention of EUR 93,900.00 and GBP 30,000.00 in total (by both HMC and the RGP).

228. Although the tools and mechanisms are in place, over the review period there has been no recovery/retention of false or undeclared cross-border movements of currency and bearer negotiable instruments. Consequently, no sanctions were imposed for false or undeclared movements.

229. The existing tools, mechanisms and declared policy suggest that confiscation is among the policy objectives. This notwithstanding, concerns remain as to how well these mechanisms were applied in practice as overall results with regard to the confiscation of criminal proceeds were low.

3.4.2. Confiscation of proceeds from foreign and domestic predicates, and proceeds located abroad

230. During the period under review there were no substantial ML cases leading to convictions and consequently no significant proceeds of ML have been confiscated. The authorities reported that EUR 1.8 million had been restrained in an on-going case where there had not yet been any charges. . In total, only two post-conviction confiscation orders were achieved;⁵¹these were for GBP 95,000 and GBP 39,000 – both cases are provided in box 7 below. To date only natural persons have been prosecuted and convicted for ML (all involved Gibraltar predicates) and there has been no confiscation of assets held by intermediaries or corporate structures.

231. HMC has achieved tangible results in obtaining the forfeiture of tobacco and instrumentalities under the 1997 Tobacco Act. Over the period 2014 – 2019, a total value of GBP 741,518.00 of tobacco and instrumentalities were forfeited. It should be noted that the Tobacco Act only applies to the forfeiture of tobacco when smuggled and instrumentalities used in that smuggling.

232. Statistics were provided to illustrate the effectiveness. There is a slight improvement in terms of the amount of confiscated or retained property over the last two years. Nevertheless, compared to both GDP and the volume of assets held in Gibraltar, the overall value of the property confiscated remains low and does not reflect the risks in a jurisdiction which is a financial centre.

Table 21: Assets confiscated 2014-2018⁵²

Value of Tobacco and instrumentalities confiscated (as per Tobacco Act)	Cash seizures	Conviction based confiscation	Civil Recovery	Total
741,518.00	113,870,00	130,428.00	0	985,816.00

233. The low number of confiscation orders appears to stem from the fact that the LEAs’ main focus is on domestic predicates. There is a lack of investigations into complex schemes potentially involving services and products provided in Gibraltar for assets coming from abroad. The authorities advised that this has changed and that now they tend to focus on more complex cases

⁵¹ GBP 90,000 confiscation order was awarded in May 2019 few weeks after the on-site.

⁵² These figures are joint RGP and HMC statistics and include cash seizures, POCA conviction base confiscation and Tobacco Act forfeitures, all together

which involve money coming from abroad. To support this statement, the authorities referred to a case involving a local TCSP (please see the case summary for ‘Operation Exodus’ under IO7), in which any confiscation order will be determined by the court in the near future⁵³.

BOX 7 – CASE STUDIES (conviction-based confiscation, period 2014-2019)

Case study 1 - Operation Flame

The Defendant entered a guilty plea to one count of false accounting and one count of ML. The Defendant used fraudulent documentation, including pay slips, to open an account at a local bank. These purported to show that he was employed at his sister’s tobacco shop. He made cash payments (suspected to derive from tobacco smuggling) into the account on diverse occasions amounting to GBP 15,000 in all. . Converting cash into what were disguised as legitimate bank deposits was recognised by the LEA as the first stage of ML.

The Defendant was sentenced for ML (conversion) to a high-level Community Order requiring him to undertake 240 hours of unpaid work.

The terms of the confiscation order (under ss. 35 and 36 of POCA) were agreed with a benefit figure of GBP 46,928.59 and an order that the defendant pay GBP 39,428.59 (this being the realisable amount).

Case Study 2

The Defendant in the drugs case mentioned at Box 4 in IO7 entered guilty pleas to drugs changes and to a charge of ML which was separately indicted. He was found to have benefitted from his criminal conduct in the sum of GBP 100,375 and ordered to pay GBP 95,000 – that being the amount of his realisable assets.

234. The RGP’s statistics suggest that the majority of financial investigations they have conducted were related to drugs trafficking, fraud and tobacco smuggling.

235. The figures covering period 2016-2018 in Table 18 below show that only a small number progress to a confiscation at Court: 25% of financial investigations were not completed due to insufficient resources; 34% of financial investigations did not proceed to confiscation due to other factors (no property found, no benefit from crime, acquittals, etc.). A further 34% of financial investigations conducted during the period are pending completion of the investigation and/or the court process. Considerations with regard to the number of predicate crimes and follow up financial investigations were also discussed under IO6 (see paragraph 131).

Table 22: RGP Reasons for non-completion of financial investigations



236. The RGP and HMC are the two LEAs in charge of financial investigations. Capacity building in both of these agencies has intensified in last two years – 3 officers from RGP and 3 from HMC

⁵³ A GBP 90,000 confiscation order was awarded in May 2019, a few weeks after the on-site.

have received specialised training on financial investigations and asset recovery with the UK's National Crime Agency. Both the RGP and HMC have developed financial investigations guidance for their officers; these are brief documents defining different steps which need to be undertaken when carrying out such investigations: 13 point check lists are included in both agencies' documents and investigators are required to check them when tracing the property of an individual or related legal entity. It needs to be noted that this list is constantly under review by LEAs (e.g. RGP now has access to the Land Property database to search by address, whilst search by name still requires the DPA route). These check lists are not intended to be the sole guidance notes for investigators, and it is made clear that officers are encouraged to draw upon all aspects of their experience and training.

Table 23: Check lists

Authority/Entity	Nature of data available	Method of obtaining data
ITO	Registered for tax purposes	DPA
ETB	Employment history	DPA
Aquagib	Registered account holder and payment history	DPA
Gibelec	Registered account holder and payment history	DPA
GoG Housing Dept	GoG residency and rent value	DPA
Previous Convictions (RGP)	Previous convictions	Internal database search
MVT	Motor vehicles	Internal database search
Port Dept	Pleasure craft	DPA
Maritime Authority	Ships	DPA
Land Proerty Services Ltd	Real Estate	DPA
Companies House	Registration of legal persons	Internal database search
Customs/RGP	Intelligence	Internal database search
GFIU	Intelligence	Email request
Bank Accounts	Bank account details (26(4))	Request via GFIU

237. The Table above suggests that the authorities would pursue provisional measures against a variety of assets including funds, residential and commercial real estate, vehicles, luxury vessels and secure them before the court decides on confiscation. The authorities also advised that property of equivalent value would be seized. However, the effectiveness in this particular field is yet to be demonstrated. In addition, the authorities are confident that the legislative and institutional reforms undertaken in the last two years will soon bring more tangible results. When they are at a point at which they proactively and consistently conduct parallel financial investigations, this will not only increase the amount of property confiscated but will also create a dataset which can be examined for trends and typologies. The LEAs make requests of the GFIU and the GCID when carrying out financial investigations for any intelligence they might have about the suspects or other relevant parties. This practice also applies to cash seizures. The GFIU and the GCID are asked if they have any intelligence on the sources of funds, or about previous offending (typically tobacco and drug related) and whether a suspect's name appeared in any previous investigation/STR.

BOX 8 – Case Study (assistance provided by GFIU targeting proceeds of crime)

A STR was submitted to the GFIU about an unknown individual opening four accounts in an online bank in Gibraltar using fake identities and using forged documents to hide his true identity. Three accounts were opened using three different Brazilian ID documents and three different proofs of address. The three accounts opened were each loaded via Skrill with a large amount of US Dollars (suspected criminal property) and later exited to an external bitcoin address. The same behaviour was present with a fourth account which

was linked to the other three by shared internet protocol addresses. The authorities issued a “no consent” order under s. 4 (1)(d) POCA prohibiting the institution from paying out the remaining balances in the four accounts. The sum of USD 18,610.00 was seized and frozen with a view to obtaining a civil recovery order under s. 72 POCA.

238. Whilst only 2⁵⁴ conviction-based confiscation orders have been imposed in Gibraltar in the review period, cash seizures have been more frequently and successfully applied. This mechanism, introduced by POCA, considers the property obtained through unlawful conduct as recoverable property only if it is held by a person who obtained the property through unlawful conduct. The minimum amount specified for the ‘recovery of cash in summary proceedings’ is GBP 1,000 with a hearing required within 48 hours of its retention.

239. Since April 2017, the cash seizure provisions have been used in 31 cases by HMC. A total of EUR 93,900.00 and GBP 2,000.00 has been confiscated, whilst EUR 15,000.00 are still pending the court proceedings. The RGP has, so far, carried out 4 cash seizures with GBP 28,000.00 seized. A case example of cash seizure is provided below.

BOX 9 – Case 3 (cash seizure)

A local resident was arrested by HMC for possession and storage of a commercial quantity of cigarettes without a licence. On a separate occasion, he was stopped at the border and found to be carrying cash that, during a civil interview, he admitted was linked to the export of tobacco into Spain.

He was found guilty and sentenced to three months imprisonment (suspended for two years) and fined GBP 15,000.

The retention of the cash under an administrative forfeiture was never challenged.

A separate financial investigation was conducted, and the individual’s assets ascertained. The authorities took the view that there was no evidence of ML.

Seeking assets abroad, 3rd party confiscation

240. There have been, so far, no cases where Gibraltar initiated the seizure or confiscation of assets which were in or had been moved to other countries.

241. In very few cases have LEAs made inquiries about criminal property moved abroad or about criminal property generated by foreign predicates being held in or managed in Gibraltar. When such international inquiries have been made in the investigation phase, the first step has been to use the assistance of the GFIU. The cases on this topic presented to the assessment team involved communication with the Spanish authorities, primarily by HMC attempting to trace assets abroad in relation to duty evasion. No concrete results have been achieved so far as in none of these cases were any responses to intelligence/MLA requests, requested by Gibraltar authorities, received.

242. In one case, the RGP provided valuable assistance to the Czech Republic in tracing and recovering assets during the investigation of a fraud. Details of the case are provided below.

BOX 10 – Case 4

The RGP initiated an investigation that required the involvement of the Czech Republic Police (District Police Directorate Prague) which began in June 2015. This was a parallel investigation into fraud by false representation/theft (in Gibraltar) & the ML of the proceeds of that fraud amounting to GBP 350,000.00 (in the Czech Republic). An unknown person in June 2015 hacked into the email account of the complainant and sent fraudulent emails to a Gibraltar management company authorising 3 separate transfers from the bank

⁵⁴ Few weeks after the on-site third conviction-based confiscation was obtained.

account held at a Gibraltar based bank, to an account at a bank in Prague in the name of Mr PT (with an address in London). The IP addresses of the fraudulent emails were in Washington State where the Microsoft servers were located. PT proved to be a fake identity.

Two Nigerian nationals residing in the Czech Republic were arrested there. After interview they were charged with ML offences. The RGP in consultation with the OCP&L agreed that that as the two Nigerian nationals were to be dealt with by the authorities in the Czech Republic no criminal proceedings need be instigated against them in Gibraltar. Each received a suspended sentence of imprisonment (30 and 36 months) by the First Instance Court.

The victim received approximately GBP 90,000.00 in compensation through the courts in the Czech Republic, this being the amount confiscated from the defendants. The remaining GBP 260,000.00 had been removed from the Czech Republic to bank accounts in China, the USA and Sweden. That amount has not yet been recovered by the Czech LEAs. The victim has received an additional GBP 150,000.00 from the Gibraltar management company in an out of court settlement.

243. Given the jurisdiction's role as an international financial centre in which Gibraltar's financial services and products are routinely used, many structures will have involved foreign companies and foreign natural persons. There will be instances where there are suspicions particularly in cases in which there is a question in respect of the source of funds. This is acknowledged by the authorities.

244. Gibraltar has not received a request for the seizure and confiscation of the proceeds of crime from a foreign jurisdiction. The authorities argued that criminals did not tend to keep their assets in Gibraltar as it was quite difficult to conceal such assets in such a small community where they would be noticed easily and then targeted by LEAs or other institutions. The assessors cannot agree with this argument – a financial centre would attract assets that could be laundered discretely through financial products and services rather than through expensive real estate or luxury vessels. Whilst a joint investigation team (JIT) could be set up in cooperation with other EU jurisdictions Gibraltar has not received or made any such request for the purpose of a financial investigation to date. It was advised that JITs could be established even with non-EU member states but this has not been tested.

245. Overall, the absence of any large-scale ML investigations involving the tracing of assets held or managed by Gibraltar intermediaries or corporate structures, and triggering further investigations into such assets held in similar structures abroad, suggests that this element of IO8 has yet to achieve tangible results.

246. No formal arrangements for asset sharing are in place. The authorities indicated that with the EU member states they would apply a 50-50 principle - when the value exceeded EUR 10,000 half of the sum would be allocated to the Gibraltar budget and the other half to the requesting State. If it was less than EUR 10,000 the amount would be considered as part of the revenue of Gibraltar. With states outside the EU asset repatriation and sharing would be dealt with on a case by case basis. The apportionment would depend on the circumstances of the particular case. Since no case examples have been provided, the assessors have not been able to assess the effectiveness of these arrangements.

247. Post-conviction confiscation investigations regularly include the recovery of the property (or the value of the property) held by 3rd parties. Given the focus on predicate criminality (such as drug trafficking or tobacco smuggling,) the recovery of property held by 3rd parties typically concerned a motor vehicle or a motorcycle transferred by the Defendant into the possession of relatives or friends in an effort to put it beyond the reach of the authorities. The RGP suggested that the vehicles that were seized during their investigations were not of significant value and thus any value they might have realised if sold is not reflected in the overall table of assets confiscated.

248. Both the RGP and HMC considered it important to seize and confiscate instrumentalities. Although during the interviews the LEAs had a good understanding of how to pursue instrumentalities, this topic was not included in the Standard Operating Procedures for financial investigations. No statistics on the number or value of instrumentalities seized were available at the time of the on-site visit. There were several cases reported in which computers had been forfeited as they had been used in the commission of the crime. The same was true of any boats or other equipment used in smuggling tobacco. Although in tobacco cases the amounts recorded did not clearly distinguish between the value of tobacco seized and the value of the equipment used to smuggle it, the assessors were assured that the instrumentalities in these tobacco cases were always forfeited.

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

249. HMC is in charge of the cross-border seizure of cash and BNIs. Since Gibraltar’s land border with Spain is not an external EU border, the requirement to submit a Cash Declaration at an external EU border for amounts of EUR 10,000 and above does not apply. There is however an obligation to declare such amounts of cash to the Spanish authorities as a result of Spanish border policy.

250. Gibraltar’s port and international airport enable border crossings with non-EU member states. Both airport and port border crossing points have areas where passengers are required to declare cash where the amount is EUR 10,000 or more. This system has been in place since March 2018. The first declaration was submitted in October 2018 and was followed by 50 more in the first three and a half months of 2019.

251. The officers in charge are trained in detecting where there has been a failure to declare cash or a false declaration in respect of cash. Trained cash detection dogs are also used.

252. Despite the measures undertaken so far, HMC only presented cases of cash seizure at entry points, in particular at the land frontier with Spain. No cash or BNI has been seized/confiscated as a result of the detection of a false declaration or undeclared cash. Consequently, no penalties could have been imposed.

Table 24: Cross border transportation of currency and bearer negotiable instruments

Year	Number of declarations or disclosures				Suspicious cross border incidents			Assets restrained (amount in EUR)
	Incoming		Outgoing		Suspicious of ML	Suspicious of FT	False declarations	
	Currency	Bearer negotiable instruments	Currency	Bearer negotiable instruments				
2013	Nil	Nil	Nil	Nil	Nil	Nil	Nil	Nil
2014	Nil	Nil	Nil	Nil	Nil	Nil	Nil	Nil
2015	Nil	Nil	Nil	Nil	Nil	Nil	Nil	Nil
2016	Nil	Nil	Nil	Nil	Nil	Nil	Nil	Nil
2017	Nil	Nil	Nil	Nil	Nil	Nil	Nil	Nil
2018	1	Nil	Nil	Nil	Nil	Nil	Nil	Nil
2019	37	Nil	13	Nil	Nil	Nil	Nil	Nil

253. In the absence of any case examples the assessment team finds it difficult to assess the effectiveness of this particular core issue. The authorities provided the assessment team with their views as to why these returns were so low: the majority of passengers travelling in and out of Gibraltar to Morocco (a non-EU MS) via plane or by a ferry are persons of Moroccan descent who are resident in Gibraltar and visiting their families across the Straits. Having worked in Gibraltar, these persons travel to Gibraltar to collect their pensions. The other air passengers are mostly tourists, usually British (sometimes on connecting flights) and Spanish families, and on occasions locally organised tours. Business travellers are infrequent. The nature of such travellers' trade will have been questioned by HMC and verified through the documentation provided; there has been nothing to suggest that large quantities of cash are being transported. Both tourists and businesspeople very rarely travel to Morocco by ferry from Gibraltar but instead tend to opt for the Algeciras and Tarifa ferries that depart nearby from Spain with greater frequency. Whenever tourists or businesspeople are seen on board, they are easily recognisable and are often challenged.

254. Gibraltar Port Authority data is regularly analysed in order to scrutinise vessels arriving in Gibraltar which are sailing to or from ports that lie outside the EU. These analyses confirm that payments for commodities purchased in Gibraltar are prearranged and pre-paid by shipping agents and conducted through bank transfers. The master of such a commercial ship may engage in paying the crews' salaries (in cash) whenever a member of crew leaves the vessel after his/her contract expires or his/her tour terminates. The authorities advised that the cash for this purpose is generated locally in Gibraltar through a shipping agent. The standard journey arranged for these crew members is a flight between Gibraltar and London. Because flights to the UK are considered to be within the EU's internal borders, there is no requirement for cash to be declared when leaving Gibraltar.

255. It was stressed that shipping agents, maritime companies and their captains have been advised by the authorities (and advised in writing) of the need to declare the cash when entering and exiting Gibraltar waters.

256. With regard to pleasure vessels, the obligation to declare very much depends on the vessels previous or next port of call. Many transatlantic journeys often include stops in the Azores or the Canary Islands before or after stopping in Gibraltar. Much of the travel to and from the East of the Mediterranean, usually at the start and end of the summer season respectively, will involve stops at other EU ports.

257. The authorities also advised that HMC Marine and Outfield crews have been tasked with increasing the number of searches of vessels for undeclared cash with the assistance of the Cash Detection Dogs. The 2018 NRA analysed the ML/FT risks deriving from the cross-border movement of cash and found them to be very low.

258. The assessment team can, in part, agree that some of the arguments advanced by the authorities explain the absence of cash/BNIs moved across the border. One of the examples why the assessment team believes that results in this area do not fully reflect the risks is the frequency with which ships and luxury vessels enter the port of Gibraltar to refill their oil tanks (the price of oil is lower in Gibraltar than in Spanish ports). HMC has strict rules on which documents/certified statements the crew and each vessel needs to have when entering Gibraltar's waters, which are regularly checked. The information on any oil purchase is kept by the OFT. Even if most oil purchases are carried out by shipping agents through bank transfers, this does not mean that there would be no oil purchases made in cash. Luxury goods available in Gibraltar such as expensive watches and jewellery might also be bought with cash. The HMC advanced that any company paying over GBP 8,000.00 in cash for oil or any other item would need to declare that cash

purchase through the cash declaration system. Given these scenarios one would expect that more declarations would have been made. HMC had not received from the OFT information in respect of any cash purchases of oil. A more in-depth analysis of the risks posed by the cross-border movement of cash is needed. In view of this, the assessment team is of the opinion that the results of the seizure/confiscation of cash/BNIs transported across borders are only partially in line with the risks.

3.4.4. Consistency of confiscation results with ML/FT risks and national AML/CFT policies and priorities

259. The confiscation results achieved so far by Gibraltar do not sufficiently reflect the assessment of ML/FT risks and national AML/CFT policies and priorities. The authorities have only recently started conducting financial investigations systematically and as a high priority criminal justice policy objective. As already noted, the results achieved to date are far lower than what might be expected from an international financial centre – even when Gibraltar’s small size is taken into account. The authorities are to be commended for their effectiveness in executing cash seizures and Tobacco Act forfeitures of tobacco but there is a shortfall in the use of conviction-based confiscation and civil recovery proceedings. Two⁵⁵ conviction based confiscation cases (both for predicate offences committed in Gibraltar), the absence of confiscation orders deriving from prosecutions in large scale ML schemes with predicates committed abroad and no civil recovery cases yet completed are further points confirming that the areas where criminal assets should be actively pursued have not been focused upon by Gibraltar LEAs. The authorities have also not proactively sought cooperation from their foreign counterparts in order to restrain and seize assets located or moved abroad. The main focus has been on seizures and confiscation in respect of local predicate offences.

260. The LEAs acknowledged that Gibraltar, being an international financial centre, with a significant volume of assets held by FIs for corporate structures, is expected to achieve more tangible results in this area. In that regard, they contend that some of the recent cases (e.g. ‘Exodus’ see IO7, Box 6) will in the future be more representative of the cases pursued and thus bring more tangible results.

261. As already noted, the assessors were also concerned at the lack of usage of the non-conviction-based asset recovery regime (civil recovery under POCA) given that it presents an alternative way of depriving criminals of their assets when there is insufficient evidence to prove guilt to a criminal standard. Many factors which impede conviction-based confiscation would not apply in civil recovery cases.

262. As stated above, the confiscation results achieved so far by Gibraltar do not sufficiently reflect the assessment of ML/FT risks. Although the authorities may have sought funds or assets used or intended to be used for terrorism/ FT, no FT investigation resulted in the seizure of any assets or funds over the review period.

263. With regard to confiscation of falsely or undeclared cross-border movement of cash/BNIs, paragraphs 249-258 elaborate the matter and confirm that the results only partially reflect the risks in this area.

Overall conclusions on IO.8

264. Gibraltar is rated as having a low level of effectiveness for IO.8.

⁵⁵ This conviction-based confiscation took place right after the on-site and concerned the unlicensed financial activity. This footnote is also relevant for para 234 which refers to the same case (i.e. ‘Operation Exodus’).

4. TERRORIST FINANCING AND FINANCING OF PROLIFERATION

4.1. Key Findings and Recommended Actions

Key Findings

Immediate Outcome 9

- a) Gibraltar has recently updated its CFT legislation (predominantly the Terrorism Act 2018) and has equipped LEAs with tools and mechanisms to counter the financing of terrorism.
- b) There has not yet been a T/FT prosecution in Gibraltar. Although the LEAs demonstrated an understanding of potential FT pathways that may occur in a financial centre, the relative lack of FT related STRs considered against the backdrop of transactions with conflict zones and high risk jurisdictions raises concerns as to whether the absence of FT prosecution is in line with the jurisdiction's risk profile.
- c) The LEAs have carried out several FT related investigations, all except one of which were triggered by STRs. FT investigations are given priority and the authorities observed that if there were to be a CT investigation it would always be accompanied by a parallel financial investigation. Although in some FT investigations potential avenues have not been pursued as fully as they might have been, the authorities assessed a number of potential FT activities where, for example, internet gambling and pre-paid cards may have been used for FT.
- d) Gibraltar's investigation of suspected FT adopts and is integrated with the UK's national CT strategy. It draws upon the close working relationship with the UK's law enforcement and security services and the experience, specialism, resources and expertise they provide in considering any FT related SARs, incoming FT MLA requests and activity in respect of high-risk jurisdictions. That said, where information has been disseminated to the UK authorities there are occasions where it might have been analysed further (even if subsequently) by the Gibraltar authorities.
- e) Any sentence imposed for FT in Gibraltar would follow the sentencing guidelines in England and Wales. The sentencing principles in FT cases in England and Wales are well developed and the sentences imposed in the UK are effective and proportionate. The judiciary confirmed that Gibraltar would follow the same guidelines.
- f) Some cases of FT investigations which did not result in prosecution due to what the authorities determined to be an insufficiency of evidence were pursued through disruptive procedures.

Immediate Outcome 10

- a) Gibraltar currently has a comprehensive legal framework governing targeted financial sanctions (TFS) for FT. However, the new regime came into force only before the on-site visit, rectifying a number of identified deficiencies hampering the effectiveness of Gibraltar's TFS regime throughout the reporting period. The relevant UN sanctions are now automatically applied in Gibraltar and the private sector is obliged to screen the UN designation lists. Supervision of FT-related TFS does not form part of the OFT and the RSC activities. Awareness of FT-related TFS in large FIs is higher compared to the non-financial sector which has a less developed understanding of its obligations. Although the new legislation has introduced the legal gateway for many new mechanisms, standard operating procedures have not yet been introduced.
- b) Gibraltar has identified the subset of NPOs falling under the FATF definition. The outcomes of

the NPO specific NRA have been communicated to the sector. Most of the mitigating actions related to the risks faced by the NPO sector have been finalised. The NPO statutory bodies have a limited engagement with the GFIU, the GCID, LEAs and other state agencies, which does not allow them to appropriately assess new applicants and monitor activities. Some of the NPOs interviewed appeared to be unaware of the CFT measures in place and potential ways of NPOs' abuse for FT purposes.

c) No funds or other assets have been frozen in relation to designated persons or entities under the FT-related TFS regime. Nevertheless, the GFIU has received STRs concerning potential matches with the UN-sanctions lists, which adds to the effectiveness of the FT-related TFS regime. The authorities have classified the vast majority of these STRs to be false – positives.

d) The measures undertaken by the competent authorities of Gibraltar are consistent with the jurisdiction's overall FT risk profile. The relevant NPO statutory bodies did not reveal any indications of abuse of the NPO sector for FT purposes. There have been no NPO-related information requests by foreign competent authorities, or STRs filed. The authorities have not received a MLA request concerning FT matters within the review period. There have been no FT prosecutions or convictions.

Immediate Outcome 11

a) The measures in place with regard to proliferation financing (PF) are identical to those applied in relation to FT-related TFS.

b) Gibraltar has not frozen any assets or transactions as a result of PF-related TFS. There are no PF-related STRs.

c) There is no mechanism for coordination and implementation of policies and strategies to counter PF in Gibraltar.

d) In comparison to the FT-related TFS the awareness of PF related TFS within the private sector is low, particularly among DNFBPs. Most of FIs screen against all UN lists on automatic or semi-automatic checks for UNSCR updates, relying on commercial databases.

e) The authorities have indicated that the PF risk in Gibraltar is relatively low. This is also supported by the fact that Gibraltar is not a weapons or dual use goods producer and its port mainly serves as a transit point. HMC oversees the movement of dual use goods over the borders and provides and monitors export licenses. Among supervisory authorities, only the GFSC has taken some concrete actions in regard to the supervision of PF-related TFS.

Recommended Actions

Immediate Outcome 9

a) The Gibraltar authorities (both LEAs and prosecuting authority) should formulate and/or further refine their policies and/or guidance documents on FT investigations and prosecutions, setting out the range of circumstances in which a FT investigation should be commenced and the types of evidence likely to be required in a FT prosecution. Such policies and/or guidance documents should reflect the full range of FT risks likely to be encountered in Gibraltar. These should pay particular attention to the potential misuse for FT of Gibraltar's international financial services and products and how these might be attractive to terrorist financiers, in particular the TCSP sector, Pre-paid cards, Gambling, Distributed Ledger (DLT) and Initial Coin Offering (ICO).

b) The Gibraltar authorities (with the assistance of the NTFIU if it is available) should continue its research into the misuse of these products by those engaged in FT and how that misuse might be

detected. Sector specific FT guidance should be provided by the authorities to different FIs and DNFBPs to include risks/potential risks in transactions with conflict zones and other high-risk jurisdictions.

c) The authorities should continually analyse financial inflows and outflows through the Gibraltar economy and reassess the risks, taking into account from where funds actually originate and to where funds are actually sent. Of particular interest is where funds are received from or are transferred to high risk jurisdictions or areas which border and/co-operate with such jurisdictions.

d) CT and ECU of the RGP, HMC and GFSC should continue to stay in step with the changing international environment in relation to FT by, inter alia, maintaining close contacts with their partners from the UK and other foreign jurisdictions.

e) Gibraltar should consider adopting a more unified strategy targeting specific FT risks and identifying and developing any typology observed.

Immediate Outcome 10

a) Gibraltar should introduce and effectively implement standard operating procedures for the new mechanisms introduced by the Sanctions Act 2019, among others: the identification of targets for designation / listing, processing of incoming requests, processing of outgoing requests related to freezing of funds, de-listing, and granting exemptions. This recommended action should also cover PF-related TFS.

b) The competent authorities should conduct further outreach to FIs and DNFBPs in relation to their compliance with obligations under the FT-related TFS regime. In this context, further steps should be taken to ensure that designations and amendments to the FT TFS regime are immediately communicated to all REs. This RA is also applicable under IO.4.

c) Powers for the NPO statutory bodies which will allow them to dismiss unfit trustees; exchange information with other domestic agencies; and cooperate with foreign counterparts should be introduced in the Charities and Friendly Societies Acts.

d) FT related TFS should form part of the supervisory activities of the OFT and RSC in practice. Inspections should include the verification of compliance with such obligations, especially with respect to the implementation of TFS without delay.

e) Competent authorities conducting supervisory activities should ensure that the screening of entities against the UN sanctions lists includes entities already existing in the REs databases and assets are frozen where necessary.

Immediate Outcome 11

Gibraltar should:

a) establish a mechanism for the coordination and implementation of policies and strategies to combat PF;

b) ensure that all FI and DNFBP supervisors receive appropriate training, understand the risks entailed by sanctions evasion and adequately supervise and monitor PF-related TFS;

c) provide guidance to REs specifically on the implementation of the PF-related TFS regimes;

d) conduct further awareness-raising activities in order to enhance the knowledge and understanding of the private sector on PF-related TFS obligations;

e) a more consistent approach should be adopted by all supervisory authorities when verifying

the implementation of PF-related TFS during the exercise of onsite/offsite supervision;

f) ensure that LEAs responsible for the implementation of PF-related TFS have adequate human resources with PF expertise.

265. The relevant Immediate Outcomes considered and assessed in this chapter are IO.9-11. The Recommendations relevant for the assessment of effectiveness under this section are R. 1, 4, 5-8, 30, 31 and 39.

4.2. Immediate Outcome 9 (FT investigation and prosecution)

266. Gibraltar has recently updated its CFT legislation (predominantly the Terrorism Act 2018) and has equipped LEAs with improved tools and mechanisms to counter the financing of terrorism. The proactive investigation of FT is a Policy Aim set out in the Gibraltar Police Authority Annual Policing Plan. Any FT matter would be dealt with at the highest level. Because of the size of the jurisdiction, there is no difficulty in prompt communication. If prosecuted, the Prosecution would be conducted by the Director of Public Prosecutions.

4.2.1. Prosecution/conviction of types of FT activity consistent with the country's risk-profile

267. No case of FT has reached the prosecution phase so far. Several investigations have commenced but the authorities maintained that each did not result in a prosecution because according to the authorities no sufficient evidence of FT was found. It is doubtful whether it could be said that Gibraltar has had no opportunity to apply in practice and test the mechanisms and tools available to combat FT. The authorities maintain that any FT investigation conducted ran its course and did not produce sufficient evidence to charge. There has not therefore been the opportunity to demonstrate the effective prosecution of FT.

268. Gibraltar undertook a risk assessment specifically in respect of terrorist financing in November 2016 and again under the 2018 National Risk Assessment (see also IO1). The 2016 analysis found that Gibraltar only presented a low to medium risk of FT and that no specific actions were required to be conducted to mitigate the risk. In 2018 the assessment was that Gibraltar had to be cognisant of its role in attracting international financial services and products and how these might be attractive to terrorist financiers. Despite Gibraltar's regulation of the TCSP sector, Pre-paid cards, Gambling, Distributed Ledger Technology (DLT), Initial Coin Offering (ICO) and other areas, it is recognised that each presents a risk of FT – whether or not that risk may have materialised.

269. Gibraltar relies on its relationship with the UK in addressing the threat of terrorism and FT. The GFIU and the RGP maintain links with various partners and stakeholders within the UK's counter terrorism Policing Network and the UK intelligence community, as well as the UK's home office, Ministry of Defence, and the Foreign and Commonwealth Office. RGP Special Branch (SB) is able to link into both the domestic UK CT Policing network as well as into the CTPLO network. SB is responsible for Counter Terrorism Policing, and its remit includes the acquisition and development of intelligence through various methods, the monitoring of travellers at points of entry, the surveying of critical national infrastructure and the delivering of protective security advice. Amongst its responsibilities are the regular liaison with security and intelligence counterparts in the United Kingdom, Spain and, to a lesser extent, Morocco, Portugal and the U.S. The ECU of the RGP is an entity designated to deal with FT. The SB, the ECU and the GFIU have permanent communication and cooperation.

270. Three of the four officers of the ECU's MLIU have attended courses at the National Terrorist Financial Investigation Unit (NTFIU) in the UK. One officer of the GFIU has also attended a NTFIU

course and three have undergone an eLearning FT course provided by the Associate of Certified Anti Money Laundering Specialists (ACAMS). Officers from both the RGP's ECU and GFIU attended a recent Terrorist Financing Workshop on Virtual Assets in Tel Aviv to ensure that they kept abreast of potential misuse of FINTEC by terrorists.

271. Gibraltar is of course a short distance from North Africa where there may be some who are radicalised. Gibraltar has its own community of those of Moroccan origin who are well integrated and there is a small transient population of Moroccan nationals moving between Morocco and Gibraltar. Although there is always a risk of radicalisation of individuals in any population, there is no intelligence that there is a problem with so-called foreign terrorist fighters and the funding of such fighters – although the authorities are conscious that this may arise at any time. The GFIU has access to the FTF Interpol database through GCID and has ability to cross reference this against Gibraltar's Border Management System (NCICS) allowing for a dynamic identification of FTFs if they use Gibraltar as a transit point. Project Citadel is an example of an on-going outreach programme to raise security awareness and the promotion of community vigilance by encouraging the reporting of suspicious individuals and behaviours in an effort to prevent terrorist threats and networks. An individual, who had been reported for having expressed radical views on social media, was arrested and found to be residing in Gibraltar illegally. Consequently, he was then deported to Morocco (See Box 14, Case study 1).

272. The institutional and legal framework, and the programme of specialist CFT training provides a sound basis for combating FT. However, there are some doubts about the authorities' ability to effectively detect FT cases and whether the absence of any FT prosecution is in line with the FT threat faced by Gibraltar. In particular, there are reasons to conclude that some sectors (primarily banks and e-money providers) are not submitting STRs when there may be good reasons to do so. By far the greatest number of "FT SARs" come (in this order) from the insurance and gaming sectors. The number of SARs is unlikely to be an accurate index of actual risk. Because many British car insurance policies are underwritten in Gibraltar, there are numerous false positives between policy holders and terrorist suspects or persons on sanction lists. Name checks give rise to many SARs because a common first and surname may be shared by many people who are not named terrorist suspects. The use of car insurance for policy holders in the UK does not present a risk of FT. The size of the e-gaming industry and the large number of SARs it generates produced many false positives. Although chip dumping may be a way of moving money peer to peer, the licences are proactive in monitoring such practices and the risk of such peer to peer FT remaining undetected is considered to be low. Those engaged in the e-gaming industry and the Gambling Commission both recognise that more work needs to be done in identifying FT typologies within this sector. Pre-paid card products are used in a wide variety of countries. STRs result in disseminations by the GFIU to counterparts abroad. The GFIU led a multi-agency project (Project Capsa) attempting to identify whether there was any use of locally issued pre-paid cards by potential foreign terrorist fighters (some cards may not carry any enhanced due diligence). Further work needs to be done on this topic in pinpointing the location of usage and in discriminating between suspicious and legitimate usage. In 2016 one request in respect of the use of an e-money product was made of the GFIU by the UK's NTFIU. The investigation of the suspect centred on the purchase of component parts which were used in the manufacture of bombs for the IRA. The e-money provider provided the information requested immediately and the GFIU provided the information to the NTFIU on the same day as their request. The defendant pleaded guilty in the UK to the commission or preparation of acts of terrorism and was sentenced to 18 years. The urgency with which the GFIU responded is, of course, commendable but it may well have been useful for the GFIU (perhaps with any advice from the NTFIU) to have later gone back over the transaction and analysed with the e-money provider whether the transaction might have been detected as suspicious at the time. Insufficient evidence has been provided by the authorities

to establish that where FT is suspected, detected and investigated by an agency outside Gibraltar, the Gibraltar authorities have fully explored whether there were earlier opportunities for detection in Gibraltar which might have been missed.

273. One of the principle FT risks is likely to be from the use of Gibraltar (as with any international finance centre) as a transit jurisdiction for the movement of funds through the jurisdiction or for the involvement of institutions such as Gibraltar TCSPs in the management of foreign funds or businesses which are linked to terrorist activity outside Gibraltar. A significant FT threat may arise from Gibraltar's products and services being used for FT purposes by individuals or organisations anywhere in the world which have no other link with Gibraltar. An assessment therefore has to be made as to which of its services or products is likely to appeal to clients engaged in FT (or ML). The Gibraltar authorities advanced that the licensing and regulatory regime of the TCSP sector, in place since 1997, mitigated the risk of the misuse of this sector (see IO3). The AT does not consider that the fact that the TCSP regime is licenced and regulated and has been for 20 years, of itself provides a sufficient level of mitigation of risk. Confidence in a settled history of TCSP licencing and regulation can shade into complacency in respect of the ML and FT risks which might be encountered. That said the authorities noted some potential risks posed by services or products offered by the TCSP sector (please also see paragraph 275 below). A written typology was retained by the Police as to the characteristics of a TCSP which might potentially be most vulnerable: where the MLRO and Compliance Officer functions were not independent of the business side (this might be the position in smaller businesses where a few employees conducted multiple roles or where a controlling or dominant individual was the owner of the TCSP).

274. The GFSC is to be commended for collecting annual data in respect of the inflows and outflows of monies from conflict zones and high-risk jurisdictions. This data is available for 2016 to 2018 and is passed to GFIU and NCO. It is not clear to what extent this data has been used for strategic or operational analysis. Based on this data the GFSC also developed 'AML/CFT (Conflict Zones) - An assessment of exposure and vulnerabilities' – a document intended to further inform their on-site supervision programme. The assessment team considers this practice as being of particular relevance for the identification of potential FT vulnerabilities and the prevention of FT in general. In this document, the GFSC noted that "as an international finance centre, the assumption may be that Gibraltar faces an enhanced threat of being used as a conduit for financial flows intended to finance terrorism in other countries and that the analysis looks to measure the threat of Gibraltar's financial services industry used as a conduit for transactions to finance terrorism in conflict zones or other high-risk countries." With regard to high-risk countries, in 2018 Gibraltar based institutions handled a total of 38,365 incoming transactions and 335,354 outgoing transactions. The corresponding values were GBP 111,246,796 received and GBP 92,649,602 issued respectively. The banking industry was overwhelmingly the largest in terms of its exposure to high-risk countries by value of transactions. Despite the high number of transactions, no FT STR was made. The GFSC therefore questioned "whether the FT suspicious transactions' reporting is adequate." A similar conclusion may be reached with regard to e-money which, as per the 2018 NRA, poses one of the higher FT risks and where only one STR was submitted; the GFSC considered this to be "at odds with the disproportionate number of transactions linked to the high risk countries." The assessment team shares these concerns. The 2018 NRA had different approach: for payment services, it states that, although the risk exposure may be considered as quite high (given the significant amount of transactions they carried out with high risk jurisdictions and conflict zones), the sector shows a good level of awareness and is able to put in place the relevant red flags. With regard to TCSPs, the GFSC, observed that not all banking relationships were with Gibraltar banks, or even EU banks. In addition, the GFSC's "Thematic Review Report. Trust and Company Service Providers. Systems of Controls for Anti-Money Laundering and Combating Terrorist Financing (June 2018)" identified a number of shortcomings

which were not endemic to all firms but an area of concern for various firms, including: i) the use of unknown third party entities or individuals providing nominee shareholdings, where there is a lack of documented rationale, oversight and monitoring of the relationship; ii) in circumstances where the TCSP on-boards a corporate client of which the shareholder is from a non-EEA state, not verifying “whether the nominee shareholding entity or individual based outside Gibraltar is a regulated entity from a jurisdiction where similar AML/CFT requirements are applied”; iii) no due diligence being conducted on the nominee shareholder where it is an entity or individual based outside the firm or jurisdiction; iv) no documentary evidence to support the rationale for the appointment of a third party nominee shareholder, particularly when the firm itself is authorised to provide this type of service. Instances of poor practice such as these increased the risk that a TCSP operating this way would be used to enable FT and that where FT may be occurring it passes unsuspected by the TCSP, unreported to the authorities and thereby remains undetected. Again, the 2018 NRA made little use of this data to further inform potential FT related vulnerabilities of the sector and establish proper mitigating measures.

275. It is acknowledged that detecting financial flows is far from a simple exercise and that a client of a financial institution might use more than one jurisdiction for the purposes of a particular structure or transaction and the link with the source or target jurisdiction might not be readily apparent. If the scrutiny is on the underlying customer, a properly applied due diligence process should reveal the link. If it is the flow data which is being examined, it only reveals the source or destination of the immediate jurisdiction. If that source or destination is, like Gibraltar, a financial centre and is acting as an entrepot, that jurisdiction will be recorded as the source or destination even though the origin or destination of the assets is elsewhere. Where there are deficiencies in the practice operated by some TCSPs as identified by the GFSC and there is insufficient scrutiny of the customer, the nominee shareholding entity concerned or the multi-jurisdictional structure used there is an increased risk that FT will pass unsuspected and no suspicions having been engaged, no suspicions will be reported.

276. Whilst the assessment team is not in position to question the NRA’s overall conclusion that the FT risk in Gibraltar is medium to low (this might well be the case but also might not be given that important elements noted above were not thoroughly analysed in the 2018 NRA), the significant gap between the overall amounts of transactions with conflict zones/high risk jurisdictions and the number of STRs submitted by relevant sectors in conjunction with certain vulnerabilities identified in the thematic reviews indicates that some opportunities to identify and further pursue potential FT may well have been missed. For these reasons the assessment team cannot conclude that the absence of FT prosecutions and convictions is commensurate with the risks to which Gibraltar as an international financial centre is exposed.

4.2.2. FT identification and investigation

277. Over the 5-year period there have been 50 FT related SARs. Overall 14 investigations were initiated all of which (bar one) were instigated by a STR. None has given rise to a FT prosecution. There have been no MLA requests – either incoming or outgoing – in respect of a FT investigation over the reported period, nor have there been any Police to Police requests in respect of FT matters. All enquiries have been via the GFIU or to the NTFIU. The Table below provides details on FT investigations in the period 2014 – 2018.

Table 25: FT investigations 2014-2018

	2014	2015	2016	2017	2018
Number of cases investigated for FT	5	1	3	3	2
Number of individuals investigated for FT	5	1	8	5	2

Number of cases investigated for FT initiated by STR	5	1	2	3	2
Number of cases investigated for FT where information from STR was used	5	1	2	3	2

278. Out of 50 SARs forwarded to the RGP SB by the GFIU the majority (about 70%) were forwarded for intelligence purposes only. In practice, however the STRs have tended to be false positives and the subjects were non-resident: 92% of the SARs were related to non-Gibraltar residents and of these 69% were domiciled in the UK. Intelligence was submitted to the relevant jurisdiction of residence and no further investigation was undertaken in Gibraltar.

279. Almost all FT investigations were initiated by a STR. As can be observed from the cases below, in most FT related investigations, the GFIU did not identify any financial activity by a suspect in Gibraltar. The GFIU is proactive in its spontaneous dissemination of intelligence to local LEAs and other jurisdictions with a 100% dissemination rate for SARs to the UK. The examples set out below are investigations triggered by the STRs coming from different REs/sectors.

BOX 11 – CASE STUDIES

Insurance

The policy holder was interlinked to different countries: UK, Spain, Morocco, UAE and Gibraltar.

During their CDD the insurance company came across a website appearing to be trading under the same name as the company to which the policyholder had ties. This website related to the trading of weapons, the collection and transportation of explosive devices and security training. There was no evidence to suggest that the policyholder was connected with the website. Interpol checks yielded no further results. The subject resided in Spain and had no financial footprint in or ties to Gibraltar. Intelligence was spontaneously disseminated to the relevant jurisdictions by GFIU.

Accountant

A Company registered in the Bahamas with a UBO based in the UK wished to invest with a fund administrator. CDD revealed a news article suggesting that the sole director and UBO of this company had family ties to and a business relationship with a person with connections to Terrorism. A FT investigation was initiated but the subject had no financial footprints / ties to Gibraltar. The business was declined and intelligence spontaneously disseminated to the relevant jurisdiction by the GFIU.

TSCP

A TCSP during its CDD on-going monitoring identified a payment of GBP 366 made from a personal bank account outside of Gibraltar to a charity declared by the UAE as a terrorist group. The Subject was based in the UK and had no financial footprint in Gibraltar. Intelligence was spontaneously disseminated to the relevant jurisdiction by the GFIU.

Prepaid Cards

A MLRO submitted a SAR concerning two accounts registered in Turkey. The account holders used a similar pattern in their e-mail and lived at the same address, however the IP Addresses were different. Accounts had travel related transactions (flight / hotel). Further, the cards were being purchased from the same locations. The MLRO suspected that the cards/transactions could be used to facilitate the movement of individuals into

Turkey for potential terrorist activity. The Subjects were based in the UK and had no financial footprints in / ties to Gibraltar. The business relationship was terminated and the GFIU disseminated information to the relevant jurisdictions.

Gaming

During their CDD a gaming company came across information related to the subject having been arrested for importing counterfeit cigarettes. Further searches revealed that a person shown as a co-habitant at his address, with the same surname, was being sought for a GBP 1 billion tax fraud in Italy using fake companies. A press release suggested that this was for the purpose of funding terrorism. The Subject was based in the UK and had no financial footprints in / ties to Gibraltar. Intelligence was disseminated to the relevant jurisdictions by the GFIU and the business relationship terminated by the gaming company.

280. In one case (Operation Exodus, see IO7, Box 6) there was a FT investigation within a larger ML investigation, although FT charges were not ultimately brought. The male suspect was allegedly laundering criminal property for some criminal clients. One such client was found to be linked to a mosque in Russia which had links to terrorism. Enquiries through the GFIU and through the CARIN network were made to Russia, Turkey and Ukraine. The identity of this individual was confirmed, and limited intelligence was provided. (There was no disclosure by the Defendant of any knowledge or suspicion which came to him in the course of a business in the regulated sector that another had committed/ or attempted to commit a TF offence; the Defendant might have been investigated and charged with failing to disclose under s.46 TA 2018.) The GFIU made disseminations to other jurisdictions but the Prosecuting Authority took the view that there was insufficient evidence for a FT prosecution. ML charges were brought but subsequently dropped when the defendants pleaded guilty to conducting licensable activity without a licence as well as failing to conduct proper CDD and keep proper records.

281. In another case a SAR was submitted from a TCSP reporting that an UBO was trying to reinstate a company which had been struck off. This company had been incorporated in Gibraltar but owned a warehouse business in Morocco. The authorities observed at the time of the on-site visit that this appeared to be an unusual structure with no apparent legitimate commercial purpose. The same assessment might have been made (but was not made) by the TCSP concerned. At the time of the request for reinstatement, the TCSP became aware that one of the directors was serving a prison sentence in Morocco for a FT offence. To investigate whether there was any connection between the FT activity and the Gibraltar company, enquiries were made through the GFIU and through the NTFIU. The investigators' requests for specific intelligence from the Moroccan authorities were not successful. Rather than let a convicted FT own a company in Gibraltar the reinstatement of the company was prevented. This may well have been a proportionate disruptive response. It is no criticism to say that Gibraltar, given its size, has very limited FT case experience to draw upon. Again, it might have been productive with the benefit of hindsight to have scrutinised the process by which, on the information potentially available to the TCSP when on-boarding the client, the TCSP ought to have been suspicious and there were opportunities to make a submission to the GFIU which were missed at the time.

282. At present only one FT investigation has arisen as a parallel investigation to an investigation into predicate terrorism offending (please see case study below).

BOX 12 - CASE STUDY (Banking)

Intelligence from open source social media raised a suspicion of possible travel to a conflict zone by a Gibraltar resident. The RGP SB commenced a proactive CT investigation.

As part of their investigation they carried out enquiries with the GFIU with a view to identifying bank accounts with which to progress a parallel financial investigation. This caused the local bank to submit a defensive SAR. The data supplied with the SAR did not provide any evidence to support the suspicions. The investigation revealed a legitimate purpose behind the travel arrangements. No further action was therefore taken.

283. The authorities advised that any CT investigation would immediately trigger a parallel financial investigation which would be coordinated among RGP (ECU in coordination with SB) and GFIU. The Standard Operating Procedure for FT, which is developed for investigators of the ECU and SB, clearly suggests not only that but also that FT investigations should be a priority. It is possible that a parallel FT investigation in Gibraltar and elsewhere could be initiated by terrorism offences committed outside Gibraltar. It is obviously more difficult to assess risk related to activity elsewhere, especially where those funds may not be linked to a specific attack. Nonetheless the case below demonstrates an ability to investigate financial aspects when a suspicion of terrorism or a potential link to a terrorist suspect is detected.

284. The RGP considered STRs allocated to the RGP SB by the GFIU as constituting the record of that which would initiate an investigation but might also form the basis of a typology of FT types. An example of a case upon which a typology was developed is presented below.

BOX 13 – CASE STUDY (FT related SAR from accountant linked to UK resident)

May 2014. A Gibraltar based accountant was the administrator of an investment fund. The fund received a request to invest in the fund from a Caribbean registered company. The accountant's CDD on the company identified the UBO. A newspaper report (that was partly retracted) linked the UBO through family ties to two persons listed by the USA as having links to terrorism. The subject was a South African national with a UK residential address. The accountant did not accept the business and reported the matter to the GFIU. Due to the person's residential address, intelligence was spontaneously disseminated to the NCA in the UK by the GFIU. The matter was allocated to RGP SB but the subject had no other connections to Gibraltar and no further local investigation was conducted.

285. The authorities have demonstrated that they are vigilant to signs of FT coming either from GFIU intelligence reports or other sources. There has been an assessment of a number of potential FT activities using, for example, internet gambling and pre-paid cards and the authorities have applied the measures and mechanisms at their disposal. That said, the AT still questions (as does Gibraltar's GFSC) to what extent the FT ST reporting (or lack of reporting) by relevant sectors influences the effective investigation of FT. The AT is also of the view that with FT as with ML potential avenues have not been pursued in some investigations as fully as they might have been.

4.2.3. FT investigation integrated with –and supportive of– national strategies

286. Gibraltar considers that the UK National Counter Terrorism Strategy "CONTEST" is an overarching national strategy for the combatting of terrorism and specifically FT. Within this strategy FT comes under the "Pursue" pillar where amongst other objectives, the strategy aims to "maintain the use of enhanced legislative tools to target and disrupt terrorist finance". Under the "Overseas Priorities" section, the strategy aims to "*illuminate and disrupt planned attacks directed at the UK and its people or interests overseas, reduce terrorist capability, weaken the drivers of terrorism and protect and mitigate the impact of attacks*". The RGP's Annual Policing Plan (version 2018 – 2019) the Delivery Plan for the first Goal "Protecting our National Security" includes references to the UK National Counter Terrorist Strategy.

287. The Gibraltar Anti-Money Laundering and Combating Terrorist Financing Strategy (2017) makes a single reference to FT stating that the RGP's ECU/MLU, when there is an indicator or knowledge of FT activity, should prioritise work on concluding FT investigations over the other work. The FT standard operating procedure document which includes all steps that need to be taken when investigating potential terrorism financing activity also requests the ECU and SB to meet immediately, and, within a day an indication of FT was detected, to discuss investigative strategy for a particular case. The document also calls for regular meetings to be held between these authorities to review the progress made with regard to the investigation.

288. The GFIU also developed a policy document entitled 'FT Response Policy'. The document aims to provide a framework for GFIU to respond to a disclosure related to terrorism and to a request from a foreign FIU related to terrorism or a terrorist incident that may have a direct or indirect link to Gibraltar. The document also aims to ensure that i) Law Enforcement Agencies are supported by providing financial data and relationships that can assist in responding to a terrorist incident or any suspicion of FT ; ii) how Egmont systems and services (e.g. ESW) can be adequately supported and an effective response provided to matters requiring urgent attention including outside of core business hours; and iii) a consistent approach is taken in creating enhanced intelligence packages for dissemination that will assist in conducting further investigation to mitigate any potential threats to life and/ or property.

289. The assessment team took note of all these strategic documents and responses to FT. These documents provide a number of legal and operational measures – most of which have already been undertaken. One document titled, *Gibraltar Counter Terrorist Financing Framework* produced by the GFIU, is a document that sets out the arrangements in place for the collection, gathering, governance responsibility and operation of the LEAs and supervisory bodies with responsibilities for CFT. Whilst this is commendable, the authorities would benefit from a more unified strategy targeting specific risks in Gibraltar and identifying and developing any typologies observed.

290. The exchange of information between the relevant authorities involved in prevention and detection of FT is good. Supervision, intelligence and law enforcement work hand in hand and regularly share information related to FT. Numerous MoUs were signed between them. The MoUs make specific reference to the security and confidentiality of information, including the processes of their handling, storage, dissemination and protection. Nonetheless, the authorities should consider providing sector specific FT guidance for different FIs and DNFBPs to further strengthen the overall response to FT threats.

4.2.4. Effectiveness, proportionality and dissuasiveness of sanctions

291. The sanctions provided in the legislation for FT offences appear to be proportionate and dissuasive. Because there have been no FT prosecutions and convictions there is no evidence in support of whether sanctions or measures applied against natural and legal persons were effective, proportionate and dissuasive. The judiciary confirmed that in the event of any convictions for FT, any sentence imposed would follow the sentencing guidelines in England and Wales. The sentencing principles in FT cases in England and Wales are well developed and the sentences imposed in the UK are effective and proportionate.

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

292. Some cases of FT investigations which did not result in prosecution due to insufficiency of evidence were pursued through disruptive procedures. The cases presented to the assessment team refer mostly to the measures deriving from Gibraltar's Immigration, Asylum & Refugee Act. In three cases, where the lack of sufficient evidence of the suspects' involvement in FT meant there could be no prosecution, each suspect was deported from Gibraltar. Although the authorities advised that other disruptive strategies (if insufficient evidence was found of FT) would equally be applied, deportation under the Immigration Act by way of a Detention and Removal Order was the only disruption strategy effectively applied in the jurisdiction. Case studies are presented below.

BOX 14

Case study 1

A Moroccan national with a history of criminality residing in Gibraltar illegally was investigated for a CT offence relating to his alleged support for a proscribed terrorist organisation. No FT was offence identified,

and in view of the low scale of the offence in question, a disruptive route was adopted in the public interest by way of deporting him to Morocco on the authority of a Detention & Removal Order issued by His Excellency The Governor due to his irregular Immigration status in Gibraltar, under the Immigration, Asylum & Refugee Act.

Case study 2

A European national of North African origin became known to SB in 2013 following his arrest for minor violence. Enquiries overseas revealed numerous criminal convictions and potential links to terrorism and/or extremist ideology. A CT investigation identified no offences in Gibraltar. A Detention & Removal Order was obtained on the grounds of public security, and he was deported to Spain.

Case study 3

Information received from Spanish authorities suggested that a male who had been convicted of terrorism related offences had entered Gibraltar illegally from Spain. A spontaneous SB operation promptly located the subject at a local hostel, and he was detained under Immigration legislation.

A Detention & Removal Order was obtained on the grounds of public security. He was deported to Spain.

Overall conclusions on IO.9

293. **Gibraltar is rated as having a moderate level of effectiveness for IO.9.**

4.3. Immediate Outcome 10 (FT preventive measures and financial sanctions)

4.3.1. Implementation of targeted financial sanctions for FT without delay

294. Throughout the review period, Gibraltar primarily implemented TFS in accordance with the EU Council Decisions and Regulations. Nonetheless, the procedures for and implementation of TFS, as established by the EU Council Decisions and Regulations, are not effective due to the deficiencies within the framework of applicable EU regulations. TFS pursuant to UNSCR 1267 and subsequent resolutions were not implemented without delay (as required by the FATF standards) due to the delay taken to transpose UN designations into the EU legal framework. This was a serious impediment to Gibraltar's effectiveness in preventing terrorists from raising, moving and using funds. Apart from EU mechanisms, provisions for implementing TFS pursuant to UNSCR 1373 also exist in the 2001 Terrorism (United Nations Measures) (Overseas Territories) Order (art.5) and the 2011 Terrorist Asset Freezing Regulations (TAFR) (Regulation 16), although in the view of the AT no successful reliance could be made upon the Order given the UK Supreme Court judgement in *Ahmed vs HM Treasury* 2010. These mechanisms have not been exploited by Gibraltar in the reporting period. In March 2019 Gibraltar adopted the Sanctions Act, addressing the technical deficiencies in R.6 identified prior to the onsite visit. Under the new provisions of the Act, all the UN, EU and UK sanctions lists have been automatically incorporated into Gibraltar's freezing regime. This ensures the direct effect of the UN sanctions in Gibraltar (S.6(2) and S.7(1) of the Sanctions Act 2019).

295. There have been no cases⁵⁶ in Gibraltar where the jurisdiction could have demonstrated the implementation of TFS pursuant to UNSCRs 1267 or 1373, neither has it designated persons or entities that meet the designation criteria under the said Resolutions. There is no specific interagency coordination in place regarding the implementation of FT-related TFS.

⁵⁶ Although a RE identified a true match there were no freezing action taken, as no funds were deposited. See more under S.4.3.4

296. Prior to the introduction of the 2019 Sanctions Act and during the reporting period, Gibraltar relied on the EU mechanism⁵⁷ for implementing UNSCRs 1267/1989 and 1988. There was no domestic legislation supporting implementation, as in the case of UNSCR 1373 (the TAFR 2011). It was not possible for Gibraltar to propose persons or entities to UNSC Committee for designations under the 1267/1989 and 1988 sanctions regimes. As Gibraltar is not a party to the United Nations, the constitutional responsibility for proposing persons or entities to the UN listings lies with the UK. Under the new legislation, the Chief Minister is the competent authority responsible for proposing designations. The Sanctions Act (S.14) sets out the requirements for such a proposal and the necessity for coordination between the Chief Minister and the Foreign and Commonwealth Office of the UK. A MoU between the government of Gibraltar and the UK Foreign Office concerning the framework for such coordination has been signed. At the time of the on-site visit, the authorities indicated that due to the recent introduction of this new legal gateway, no standard operating procedures had yet been introduced to assume the process conducting proposals for designation, such as standard forms for listings to allow for the accurate and positive identification and proposal for designation of individuals, groups and entities.⁵⁸ Gibraltar has so far not designated any persons or entities that meet the designation criteria under the UNSC Resolutions.

297. The mechanism for the implementation of the UNSCR 1373 is set out in the Terrorist Asset Freezing Regulations (TAFR), the Terrorism (United Nations Measures) (Overseas Territories) Order 2001 and the recently introduced 2019 Sanctions Act (S.15(1))⁵⁹. The Chief Minister and the Minister responsible for financial services are the competent authorities assigned to make designations (TAFR Section 4(1)). The EU designations pursuant to UNSCR 1373 apply automatically. Although there is a legal mechanism for proposing designations, no standard procedures on intelligence gathering, sharing and decision-making are in place⁶⁰. Currently, the Chief Minister may determine a designation request from abroad within seven days of receipt of such a request (2019 Sanctions Act (S.19)), however there were no provisions to regulate the handling of such requests during the review period nor has Gibraltar received any requests to impose sanctions. Prior to the introduction of the new legislation, there were no provisions in place to regulate the de-listing and unfreezing of funds or other assets of persons and entities which do not or no longer meet the criteria for designation.

298. The mechanism for communicating designations to FIs and DNFBPs relies on the publication of links to the UN, EU, UK and domestic sanctions lists in a dedicated section of the GFIU website. Since 2018, updates to the UN sanctions list are also available to all RE through the Themis system. A dedicated tab to sanctions allows REs to download all sanctions lists via Themis. The authorities also informed that MLROs receive a notification when there is an update to the sanctions lists available in Themis. However, only few REs are aware of such a solution. Since 2019 REs are obliged to follow and use the latest version of the OFSI (UK) consolidated list, which combines the UN, EU, UK sanctions lists (2019 Sanctions Act (S.8, S.6(1) and S.7(1))). The List is updated every 24 hours. The authorities indicated, that prior to the introduction of the Sanctions Act 2019, government agencies and REs did receive updates on changes in the designations list via the Gibraltar Gazette of laws, but this did not guarantee immediate communication⁶¹. The GFSC

⁵⁷ The EU mechanism is under the EC Regulations 753/2011 and 881/2002

⁵⁸ The standard forms to request the listing of individuals/entities/groups on sanctions lists were introduced in the time frame following the end of the on-site visit.

⁵⁹ The EU mechanism is under the European Council Common Position (CP) 2001/931/CFSP and the EC Regulation 2580/2001

⁶⁰ Protocol for the Designation of Terrorists Pursuant to the United Nations Security Council Resolutions 1373, 1267/1989 and 1988.

⁶¹ The Gibraltar official Gazette is circulated approximately twice per week and it is publicly available on the web.

encourages its supervised entities to subscribe to news feeds that will send out updates to the UN sanctions lists. Subscription to news feeds is not mandatory.

299. The 2019 Sanctions Act, which was introduced shortly before the on-site visit, rectified a number of identified deficiencies hampering the effectiveness of Gibraltar's TFS regime throughout the reporting period, such as: the limited obligation to freeze all relevant categories of funds and assets; and the lack of: a) domestic legislation to support the implementation of UNSCR 1267/1989 and 1988, b) a requirement to communicate the designations to the financial sector and the DNFBPs immediately; c) reporting obligations for all types of relevant institutions; d) reporting obligations of attempted transactions; e) measures protecting the rights of bona fide third parties acting in good faith when implementing the obligations under R.6; f) a legal basis for informing the designated person or entity of the listing, its reasons and legal consequences, as well as their rights to due process, availability of de-listing procedure and access to frozen funds.

TFS understanding

300. The FT-related TFS understanding of the private sector varies and requires considerable improvement. Overall, the understanding of non-financial sector is considered to be less developed in comparison with the one of large FIs. This was confirmed by interviews held on-site with the private sector. Some REs have a mixed understanding on which "list" to screen against, referring to OFAC, FATF, whereas a few small REs (e.g. MVTs, real estate agents) are unaware of the UN sanctions lists; There were also cases where REs confused their FT-related TFS obligations with their duty to file STRs to the GFIU. This may be influenced by the fact that the GFIU serves as the first contact point for reporting frozen funds and economic resources, information regarding a designated person, and notifications of credits to frozen accounts. While filing an STR is a separate process from the immediate freezing of funds or other assets of designated persons and entities under TFS duties, it must be taken into account, that when a STR has been submitted to the GFIU based on knowledge or suspicion of ML/FT, a RE should suspend a transaction, without a notice from the GFIU.

301. Several FIs have developed their own automated screening systems (most often based on commercial software such as World Check etc.) to screen clients and BOs of customers against the UN sanctions lists. The screening is however negatively impacted by deficiencies associated with identifying the UBO by FIs (see par.376, IO 4). The representatives of financial technologies (Fintech) sector met on-site appear to be aware of their obligations stemming from the sanction regimes. As regards DNFBPs, most firms base their checks on manual open source research. Checks are often limited to new clients. The majority of market participants (especially real estate, insurance and HVD sector) screen customers against UN sanctions lists only when the customer is deemed high risk or a foreign citizen and therefore do not cover all clients. Also, screening of BOs and senior managers of corporate entities against the UN sanctions lists is not always applied by the sector's professionals and limited by deficiencies with regard to BO identification indicated in IO 4 (par.378). As regards the TCSP sector some of the entities met on-site use automated systems to screen against sanctions list, while others rely only on the official Gazette. Automated systems are also used to a wide extent by gambling operators, whereas screens are performed by the casinos when applying EDD.

TFS compliance

302. Compliance with FT-related TFS forms part of the GFSC and GGC routine AML/CFT on-site inspections. This was also confirmed, while on-site, by REs met. As regards OFT and RSC, FT-related TFS does not form part of their supervisory activities.⁶² Although the supervisory

⁶² OFT and RSC included FT/PF-related TFS in their supervisory activities as of the end of July 2019.

authorities have sanctioning powers in place, no sanctions or penalties have been imposed for failure to comply with FT-related TFS obligations. Instead, the authorities issued recommendations for remedial action. This was confirmed, while on-site, by a RE, which as a result of a deficiency identified during an inspection it received a recommendation to introduce procedures for the screening of its clients against the UN sanction lists.

Guidance

303. Interviews with supervisory authorities and the private sector suggest that limited guidance is provided on the implementation of FT-related TFS. The authorities provided information and web links in the GGC and GFSC websites where information on TFS is provided to some extent in their guidance to the industry. Prior to the on-site visit, the NCO has distributed a newsletter concerning the changes introduced by the 2019 Sanctions Act. Among other, the newsletter covered areas of domestic and international sanctions; provided a number of definitions (e.g. funds, freezing); and information on sanctions lists, reporting of hits, listing and de-listing. Due to the recent issuing of such guidance, the majority of REs interviewed were unaware of the newsletter. Throughout the review period the UK (OFSI) sanctions guidance was available in the GFIU website, although it had no reference to Gibraltar. The said guidance was replaced during the on-site visit by the Financial Sanctions Guidance Notes (11 April 2019) produced by the GFIU. These findings are consistent with the uneven knowledge of the private sector on how to freeze assets of designated persons; designee's rights, duties, and the application of exemptions from sanctions; and de-listing, unfreezing and appealing procedures.

304. Competent authorities screen their databases against the UN sanctions lists. This however refers to check against only new entries, not existing ones – when UN lists are amended. Since 2017, the NCO has conducted outreach to competent authorities to raise awareness on FT-related TFS matters.

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

305. Separately from its ML/FT national risk assessments, Gibraltar conducted a dedicated FT Risk Assessment of the non-profit organisations (NPO) sector in 2017. The assessment was conducted on the basis of qualitative information (questionnaires to the NPOs, with 50% response rate), but without validation of the responses collected, except in the form of feedback in the context of a workshop where the findings were presented. The assessment identified a subset of NPOs, which meet the requirements of the FATF definition – registered charities and friendly societies. The risk assessment concluded that the overall risk for the sector is low and that no evidence of FT abuse was found. The recommended actions identified in the FT NPO NRA were included in the post-NRA action plan. The threat of collecting and transferring funds through NPOs for FT purposes was also analysed in the 2018 NRA, where the risk was considered to be medium to low.

306. There are currently over 300 charities and 7 friendly societies registered in Gibraltar. Other forms of unincorporated associations, falling outside the scope of the FATF definition, such as clubs, societies and cultural organisations, are generally not subject to formal registration, apart from specific requirements (application for government grants, occupation of premises etc.) The vast majority of the NPOs are domestically oriented. The FT NPO NRA assessment included a recommendation to the Board of Charity Commissioners (BCC) to monitor a group of charities with higher risk indicators – NPOs providing educational grants to non-Gibraltar based beneficiaries and charities with poor system controls.

307. Charities in Gibraltar are supervised and monitored by the BCC, whereas friendly societies by the Registrar of Friendly Societies (RFS). Both authorities indicated, that they screen new

applicant NPOs. The source of funds, the economic settlor, the trustees (at least one should be local), the management of the charity, the trust deed and the objectives of the NPO are verified.

308. The NPO statutory bodies regularly monitor also previously registered charities and friendly societies, although these assessments are not FT oriented. Throughout the year, all reports provided by the supervised NPOs are reviewed (in the case of charities: income and expenditure account, a balance sheet and an annual brief activity report). Charities are subject to enquiries and checks more often provided that they have a tendency to accumulate funds instead of providing them to their beneficiaries.

309. The BCC and the RFS have proportionate, and dissuasive sanctions at their disposal in case of identified shortcomings, such as imposing fines, providing restrictions on conducting transactions or moving funds, removing of unfit trustees and staff, up to suspension of the NPO. Hitherto, such penalties have been imposed. Nonetheless, the BCC provided an example of an enquiry concerning a charity with no apparent connection with Gibraltar supposedly conducting activities in New Zealand. In fact, the NPO trustees were found to charge improperly substantial fees. As a result of the enquiry, the charity voluntarily agreed to be removed from the charities' register in order to avoid further consequences.

310. Both the supervisory authorities confirmed that amendments to the Friendly Societies Act and Charities Act would be useful, in order to introduce more proportionate remuneration, administrative fees, a more detailed application form and reflect the changing risks on NPOs abuse. The BCC supported that the power to disqualify trustees involved in serious fraud and dishonesty offences could be introduced. Both statutory bodies also underlined, that it would be beneficial for them to receive information on NPOs granted permission by Gibraltar authorities to conduct fundraising activities in cash. The need for a more flexible information exchange legal framework with other domestic authorities, aiming to assist in the course of verifying information provided by NPOs, was highlighted. The BCC and the RFS also noted the lack of a gateway to obtain information from their foreign counterparts.

BOX 15 – CASE STUDY

In the case of the Charity X, the BCC noted that in December 2018 an individual, who had been convicted of serious fraud and had been adjudged bankrupt, had been appointed as a Charity Trustee. The secretary to the Board informed the Charity X of the Board's view that this person was not fit and proper to be a Charity Trustee and he/she should be removed. In April 2019, the Board noted that this person had already been removed as a Trustee, but it nonetheless wrote to the Charity X a reminder that under the Charities Act an undischarged bankrupt is liable to be removed as a Charity Trustee. The Board notes that the Charities Act, unlike the UK Charities Act, does not contain an express provision disqualifying a person convicted of an offence of dishonesty from being a charitable trustee. The Board informed the assessors, while on-site, that it is making representations to the Government to introduce a legal provision which will provide expressly for disqualification in such cases.

311. There is no interagency co-operation and co-ordination between the BCC, RFS and GFIU, which is designated as the single point of contact for foreign authorities regarding NPO matters. This was confirmed by the assessment team during the interviews held on-site. Authorities argued that, so far, such co-operation and co-ordination is not deemed necessary. In case of suspicion of FT abuse of NPOs, none of the NPO statutory authorities is explicitly obliged under the POCA to make a report to the GFIU. However, this is covered by the legal definition of persons, which are obliged to do so (POCA S.2-4). Not all charities met on-site were aware to whom they should report a suspicious activity. No FT-related STR involving NPOs has been received by the GFIU.

312. NPOs met while on-site, expressed their need for further guidance in relation to their potential abuse for FT purposes. In 2017 a newsletter was communicated to all charities and

friendly societies providing information on a number of methodologies for abuse by terror actors. The guidance was based on the “Risk of terrorist abuse in NPOs” FATF paper rather than Gibraltar’s own analysis and thus might not necessarily apply to Gibraltar’s NPO sector vulnerability in light of the 2018 NRA findings. A workshop was also organised with high-risk charities in 2018 regarding these aspects. In 2018 a presentation concerning the FT risks of the NPO sector was delivered under the auspices of project NEXUS. Neither of the competent authorities nor the NPOs met on-site could recall any guidance issued prior to 2017. No guidance has been issued for donors. Overall, NPOs met on-site considered their potential abuse for illicit activities, including FT, to be low, primarily due to the fact that their activities are mostly domestic.

4.3.3. Deprivation of FT assets and instrumentalities

313. There have been no funds or other assets frozen in Gibraltar pursuant to the FT-related TFS regime. The authorities confirmed that they have received 13 FT STRs in total, during the review period. Mindful that the assessment team found on-site that there was insufficient awareness of internal procedures for dealing with matches (potential or real) across the private sector, in particular those stemming from the recently introduced Sanctions Act, the reporting of potential matches with relevant lists by REs adds to the effectiveness of the FT-related TFS regime. Most of the identified hits with the UN sanctions lists have been identified by authorities as false positives. Consequently, none of the investigations based on such STRs has led to FT prosecutions. During the onsite, a RE – e-money provider - indicated that it had a true match with a sanctions list, which was reported to the GFIU. The hit was associated with an attempt to register several accounts. However, no funds were deposited, thus there was no freezing action taken. Gibraltar has issued specific guidance on how REs should report funds or economic resources of designated persons. In such a case the relevant competent authority – the Chief Minister or the Minister for Financial Services – should be notified. This guidance was created on the last day of the on-site visit, therefore there was no possibility for REs to get acquainted with it.

4.3.4. Consistency of measures with overall FT risk profile

314. The measures undertaken by the competent authorities of Gibraltar are consistent with the jurisdiction’s overall FT risk profile, although the absence of a follow up on STRs connected with transfers of funds to high risk jurisdictions should be taken into account (see IO 1 par.119). Gibraltar authorities have made considerable efforts to analyse the FT risks by conducting both a dedicated FT (2016) and a NPO analysis (2017) in the NRA process, FT aspects were also included in the 2018 NRA, influenced by the EU Supranational Risk Assessment (SNRA). The BCC and RFS confirmed that the NPO sector has not been abused for FT purposes. The fact that Gibraltar NPOs are predominantly domestically oriented supports the overall low perception of FT risk. Throughout the review period, there were no incoming NPO-related information requests by foreign authorities, or STRs filed from REs. In addition, there were no incoming or outgoing MLA requests concerning FT matters, although both the RGP and GFIU have been involved in information exchange concerning potential FT. None of the conducted FT investigations had enough justification to lead to FT prosecutions or convictions. Measures envisaged in the strategy and action plan to mitigate identified FT risks have in most cases been implemented, with some exemptions, such as measures to prevent the use of anonymous pre-paid phone cards or a review of the relevant legislative provisions of the Charities Act with the introduction of necessary amendments.

Overall conclusions on IO.10

315. **Gibraltar has achieved a moderate level of effectiveness for IO 10.**

4.4. Immediate Outcome 11 (PF financial sanctions)

4.4.1. Implementation of targeted financial sanctions related to proliferation financing without delay

316. Gibraltar is an international financial centre specialised in providing banking, TCSP and insurance services to UK and other foreign customers. Gibraltar is neither a weapons manufacturing jurisdiction nor an international trade centre⁶³ or a market of proliferation goods. The jurisdiction has a port which mainly serves as a transit point. The transit is very limited to provisions and ship spares. The port mainly serves as a bunkering point. Gibraltar has no trade relationships with the Democratic People's Republic of Korea (DPRK) nor with Iran. The jurisdiction maintains an accessible shipping register that facilitate the requirement to freeze shipping assets in the context of relevant PF TFS.

317. The mechanism implementing proliferation related TFS is the same as the one for FT. Throughout the review period, Gibraltar implemented TFS in accordance with the EU Council Decisions and Regulations. The introduction of the Sanctions Act in March 2019 allows for the implementation of the UNSCR 1718 (DPRK) (Council Regulation No.329/2007, as amended, and Council Decisions 2013/183/CFSP) and the former UNSCR Security Council Resolution 1737 (Iran) (Council Regulation No.267/2012 as amended and Council Decision 2010/413) without delay. The Council Regulation (EU) 2015/1861 has introduced changes to take account of the Joint Comprehensive Plan of Action. For the period prior to the introduction of the 2019 Sanctions Act the deficiencies identified under IO.10 (including the implementation of TFS without delay) were also applicable to PF-related TFS.

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

318. The PF risk in Gibraltar is considered to be low by its authorities based on the following aspects. No cases of PF have been identified in Gibraltar and as a result no assets or funds associated with PF-related TFS have been frozen. Gibraltar has never received an international request (formal or informal) of PF activities, movement of funds or other assets. Although a connecting border is not necessarily required for the movement of funds or other assets linked to designated persons and entities, Gibraltar does not neighbour with proliferating states or had any investigations and prosecutions on PF, including in relation to border controls.

319. The GFIU maintains a dedicated web-page to sanctions (<http://www.gfiu.gov.gi/sanctions>) which includes links to the UN sanctions list. REs can access these links without any subscription requirement. All updates to the UN lists are also published in the official gazette⁶⁴. Other supervisory authorities have links directing to the GFIU website where links to sanctions lists are available, also including links to the FATF high-risk jurisdictions list. As described under IO.10 REs have access to PF-related sanctions list through Themis and OFSI.

320. Banks and large FIs conduct sanctions screening which includes PF to a large extent. However, the awareness of PF-related TFS obligations is not even across the financial and non-financial sector. The AT also observed that the awareness of FT-related TFS amongst REs is higher than the PF one. The systems in place rely on commercial databases. There were also cases where REs confused their TFS obligations with their duty to file STRs to the GFIU (see IO.10). Small FIs and the DNFBPs met have a low level of awareness of their PF-related TFS obligations. Most firms base their checks on manual open source research (see IO.10). Among interviewed DNFBPs, some

⁶³ In 2015, Gibraltar exported GBP 193,1mil. and imported GBP 510 mil., resulting in a negative trade balance of GBP 317 mil.

⁶⁴ The Official Gazette is circulated approximately twice per week and it is publicly available on the web.

rely only on the updates posted in the official gazette, which did not meet the “without delay” requirement. The majority of market participants (especially real estate, insurance and HVD sector) screen customers against UN sanctions lists only when the customer is deemed high risk and therefore do not cover all clients. It needs to be noted that the vast majority of these entities were referring to sanctions list without specifying which exact list. Whilst further inquiring the way such checks are performed by REs, the assessment team is able to confirm that few inquired REs took into account the UN PF-related lists. The compliance of the TCSP sector with PF-related TFS does not differ with the situation described under IO.10.

321. There is no mechanism for coordination and implementation of policies and strategies to counter PF in Gibraltar. Although the authorities advised that an interagency working group discussed areas such as sanctions updates, PF awareness raising and trainings on PF-related TFS in one of its ad hoc meetings held in 2018, minutes of this meeting that the assessment team had access to did not make any specific note to these points of discussion.

322. In absence of PF evidence and mindful of the Gibraltar’s port nature of activities, the AT hold discussions with HMC on the dual-use goods licensing regime, controls and volume of trade. Figures on dual-use goods were made available by HMC (see table 26).

Table 26: Dual-use goods imports

Year/Commodity	Weight (Net)
2017	
Lubricating oils (KILOGRAM)	8,255.00
Chemical products, other than lubricating oils (KILOGRAM)	23,424.18
2018	
Lubricating oils (KILOGRAM)	12,712.60
Chemical products, other than lubricating oils (KILOGRAM)	251,697.95

Table 27: Dual-use goods exports

Year/Commodity	Weight (Net)
2017	
0kg. exports	
2018	
Glaziers' putty, grafting putty, resin cements, caulking compounds and other mastics (KILOGRAM)	2.00
Tube or pipe fittings (KILOGRAM)	698.00
Other units of automatic data-processing machines (NUMBER OF ITEMS)	138.00
Parts of machines of subheading 84798970 (KILOGRAM)	1,547.00

323. HMC oversees the movement of all goods, including dual-use ones over the borders, and provides and monitors export licenses. Applications for licencing are submitted in written form and approved by the Collector of Customs. Licences are screened against the UN sanctions list. The Collector of Customs may deny a licence or authorisation on the basis of intelligence. HMC monitors potential suspect ships bunkering at the Gibraltar port. HMC also follows the UK national vessel watch list. The list is circulated to all the police community and agencies. In light of a PF-related issue, HMC will be notified by the national maritime centre of the UK.

324. Once a year HMC reports to the UN on chemical weapons movement. HMC informed that the reporting takes place via the OAC. Gibraltar usually reports on material, mainly fire-proofing material used in construction building. The complete Gibraltar dual-use goods list is incorporated to the UNCTAD Automated System for Customs Data (ASYCUDA), which is checked by a UN expert

on a regular basis.

325. Upon a PF-related alert, the public sector will be reached within ten minutes. The RGP confirmed this via the example of an advisory note related to cyber alerts, which was urgently communicated to the private sector in 2018.

326. The GCID has incorporated the UN sanctions lists in its electronic search facility. The GCID confirmed that all financial investigators have access to its search facility.

327. During the discussions held on-site it was broadly agreed among all LEAs that further training and resources are required on identification of red flags for PF and identification and classification of dual-use goods, including personnel with PF expertise.

4.4.3. FIs and DNFBPs' understanding of and compliance with obligations

328. Banks were broadly aware of their TFS-relevant obligations. However, contrary to the FT-related TFS the awareness of the private sector on PF-related TFS is lower, particularly among DNFBPs (see further analysis under IO.10). Medium-small FIs and the entire DNFBP sector cannot differentiate between FT and PF-related TFS.

329. Banks reported that their systems update daily, which will allow them to restrain transactions soon after a person/entity is designated. Large FIs maintain sanctions compliance IT systems, including screening procedures in order to identify transactions involving sanctioned persons for FT and PF. FIs such as fund managers, electronic money and bureaux de change understand their TFS obligations and use semi-automated software for sanctions screening. The representatives of financial technologies sector are aware of their obligations stemming from the sanction regimes. Fintech entities use automated and semi-automated system for sanctions screening. The representatives of the sector highlighted their daily contact with the GFSC, which also covers the application of FT/PF-related TFS. The gaming sector has the same level of compliance as described under IO.10. The PF-related TFS understanding of a substantial number of legal professionals, REAs, HVDs, and MVTs is underdeveloped. DNFBPs, in general, consult publicly available sanctions lists on case by case, depending on the results of the due diligence (challenges on verification of identity of BO highlighted under IO.4 may have an impact). TCSPs rely on controls implemented for CDD purposes. Mindful of the deficiencies related to internal procedures for dealing with matches (potential or real) analysed under IO 10, overall, mainly large/medium FIs and few DNFBPs confirmed that in case of a match with TFS sanctions lists, they will file a STR with the GFIU and refrain from performing the transaction.

4.4.4. Competent authorities ensuring and monitoring compliance

330. The authorities have indicated that the PF risk in Gibraltar is relatively low. The Chief Minister and the Minister responsible for finance are the competent authorities for implementation of PF-related TFS in Gibraltar.

331. Throughout the review period, Gibraltar implemented TFS in accordance with the EU Council Decisions and Regulations (see s.1.2.1). Compliance with PF-related TFS was relying on REs obligation to screens against UN sanctions lists and the publication of the Official Gazette. No other form of outreach (e.g. newsletters) related to updates on sanctions list was available. Since 2018 REs receive updates through Themis and they are obliged to follow the OFSI consolidated list.

332. There is no guidance on REs compliance with PF-related TFS, whereas limited training has been provided. Since mid-2017, REs have been provided, to some extent, with training on FT/PF-related TFS by the NCO. GACO has also conducted a seminar in 2018.

333. Supervisors bear the responsibility to check and verify whether REs implement PF-related

TFS. While the GFSC and the GGC, during their inspections, check compliance with sanctions-related requirements (which would include also PF), the other supervisory authorities have either just started to inspect or do not yet inspect their sectors (see IO3). No sanctions or penalties have been imposed for failure to comply with PF-related TFS obligations (see IO.10).

334. As regards interagency cooperation on PF-related TFS and sanctions screening by the authorities the same issues identify under IO.10 equally apply to IO.11.

Overall conclusions on IO.11

335. Gibraltar has achieved a moderate level of effectiveness for IO.11.

5. PREVENTIVE MEASURES

5.1. Key Findings and Recommended Actions

Key Findings

Immediate Outcome 4

- a) RE's understanding of the ML risk is overall satisfactory albeit it varies across and within the sectors. Some sectors (e.g. fund managers, DLT providers, e-money and *bureaux de change*) have a better understanding of risks and their obligations than banks, insurance and other types of FIs. TCSPs and online gambling providers have a better understanding of risks than other types of DNFBPs (e.g. real estate agents- REAs).
- b) The FT risks are not properly understood by FIs (in particularly by banks, e-money providers, and MVTSS). FIs focus almost exclusively on sanction screening, without proper consideration of transactions to high risk countries.
- c) FIs and DNFBPs that fall under the purview of the GFSC apply mitigating measures that are overall commensurate to their risks. However, risk assessment was often referred to as risk classification of the clients and not of all relevant risk factors. Some FIs (e.g. some banks) and TCSPs, dealing primarily with high net worth individuals or offering high risk services (e.g. private banking, pooled accounts or services to companies incorporated in high-risk jurisdictions) did not always demonstrate that they are taking measures that are commensurate to these specific risk factors. TSCPs do not always apply a RBA to periodic reviews of their customers REAs do not take some of the measures that were identified by the NRA to mitigate their risks.
- d) FIs and DNFBPs exhibited different degrees in applying CDD measures. While TCSPs have a good understanding of the concept of BO, this is not always the case for some other REs, including banks, particularly when complex ownership structures or trusts are involved. FIs and DNFBPs tend to overly focus on thresholds for identifying the BOs, which is an issue of concern particularly for the identification of targets for the implementation of TFS requirements. The legal framework is not clear in requiring REs to keep records on BO, as also evidenced by some of the firms' policies.
- e) FIs and TCSPs apply periodic reviews of their customers files, based on the customer risk classifications and some trigger events. However, it is not clear that on-going monitoring of the business relationships and transactions is fully understood by all FIs. This is a challenge particularly for those firms that have legacy customers with asset holding vehicles that may not generate frequent transactions.
- f) Not all firms have a good understanding of the measures that need to be applied for politically exposed persons (PEPs), particularly that establishing source of wealth and source of funds are distinct requirements. There is also a tendency to over-rely on information provided by the customer or certified by lawyers or auditors or in commercial databases in verifying the source of wealth and the source of funds, including for high-net worth clients.
- g) FIs and TCSPs have a good understanding of the STRs legal requirements and of tipping off measures. However, the number of STRs filed by material sectors (e.g. banks, e-money and TCSPs) is not commensurate with the risk that these sectors are facing and with the number of cases where clients were exited, or transactions declined on financial crime concerns. The quality of the STRs raises concerns due to the low disseminations by the FIU and the near absence of investigations triggered by STRs. The near absence of FT related STRs evidenced by the GFSC in its

analysis of transactions to and from conflict zones might increase the risk for abuse for FT. The defensive reporting in the e-money and online gambling providers and double reporting of the latter to the FIU and GGC raise concern.

h) In general firms apply internal controls and procedures to comply with AML/CFT requirements, including those that are part of the group, commensurate to their size and risks. However, AML/CFT compliance officers do not always have the appropriate level of seniority and direct reporting to senior management of the FIs of DNFBPs.

i) The understanding of TFS and their operational implications needs considerable improvement across all sectors, and particularly for smaller FIs and most types of DNFBPs.

Recommended Actions

Immediate Outcome 4

Gibraltar should:

a) Amend the POCA to extend the record keeping requirements to BOs and all CDD measures (see analysis of R11).

b) Reach out to all REs, and particularly to smaller FIs and DNFBPs to ensure that TFS regimes (both for TF and PF) are properly understood and that firms have procedures in place to implement effectively TFS.

c) With regard to the STR regime:

i. Provide sector-specific training on indicators and typologies to increase the quality of STRs and to increase the level of reporting of ML and TF-related transactions, in a way that is commensurate to the threat that Gibraltar is facing.

ii. Ensure, by way of outreach and enforcement during the inspections that gambling firms report only to the FIU and not also to the GGC, and that firms' internal procedures are aligned accordingly. The GCC should discontinue the inbox for the collection of STR-related information.

iii. Increase awareness across all sectors on the legal framework applicable for the provision of additional information to the FIU.

d) Ensure that all firms understand that risk assessment is not only related to customer risk profiling and ensure that they systematically conduct and document a ML/TF risk assessment at firm level considering the customer base, products and services provided and the size of the firm. Ensure that firms factor in the risk classification of their customers also risk factors concerning the BO.

e) Ensure, by way of outreach and enforcement during the inspections, that BO-related requirements are properly understood.

f) Ensure that all REs understand their PEP-related requirements, and particularly that establishing the source of wealth and funds are two distinct requirements.

g) Conduct a review of compliance arrangements to ensure that ML reporting officers are appointed at management level and have direct reporting lines to senior management. Assess to what extent outsourcing compliance arrangements are justified by the size of the firm and satisfy the fulfilment of the AML/CFT obligations.

h) Authorities should consider issuing sectoral guidance to clarify what are the triggers for the

application of AML/CFT requirements to firms (e.g. online gambling and e-money providers) that provide cross-border services (particularly preventive measures and reporting requirements), including the reporting of STRs.

336. The relevant Immediate Outcome considered and assessed in this chapter is IO.4. The Recommendations relevant for the assessment of effectiveness under this section are R.9-23.

5.2. Immediate Outcome 4 (Preventive Measures)

337. For the reasons of their relative materiality and risk in the Gibraltar context, implementation issues were weighted (see also the section on Materiality and level of ML/FT risks of the different FIs and DNFBPs under Chapter 1):

- **most significant** for the banking sector and the TCSPs, which play a dominant role in Gibraltar in terms of assets, number and typologies of clients; in the case of TCSPs, also because of the types of services offered, which involve creation and management of complex corporate structures and trusts;
- **significant** for e-money providers and remote gambling operators, based on the high number of customers, mainly non-resident, the high volume of transactions, the non-face-to-face nature of the business; and specifically for the remote gambling operators, also the use of cash at betting and for topping up gambling credit; real estate agents, funds administrators and managers, insurance sector, *bureaux de change* and legal professionals (lawyers) based on size of the sector in terms of funds (funds administrator and managers and insurance) and in general for their exposure to ML/FT risks;
- **less significant** for other types of FIs and other types of DNFBPs, for the size of these sectors and the types of products and services offered. Although DLT providers were identified by the NRAs as posing a higher risk, for the purpose of the analysis of IO4 the AT considers them to be less significant, given the relatively small size of the sector in Gibraltar.

338. Assessors' findings on IO.4 are based on interviews with a range of private sector representatives, as well as on the experience of supervisors and other competent authorities concerning the relative materiality and risks of each sector. The assessment team grouped the obliged sectors into categories in terms of their significance for the overall picture of compliance.

5.2.1. Understanding of ML/TF risks and AML/CFT obligations

Financial Institutions (FIs)

339. FIs have satisfactory understanding of their sectoral ML and FT risks, and of the risk faced by Gibraltar as an IFC, albeit with varying degrees across the different sectors and within the sectors, depending also on the size and types of products offered. Some sectors (e.g. fund managers, DLT providers, electronic money and *bureaux de change*) exhibited overall a better understanding of their risks than banks, insurance and other types of FIs. This better understanding by these types of FIs appears to be based on a thorough knowledge of the relevant risk faced by the sector and of recent efforts taken by the sectoral supervisors (particularly by the GFSC), rather than being based on NRA results.

340. In general, the FIs are knowledgeable of the findings of the 2018 NRA except for the money lenders. With very few exceptions, FIs are generally not aware of the findings of the 2016 NRA, and not always aware of the FT and NPOs risk assessments, despite their being relatively recent. The

main types of FIs (banks, e-money providers and fund managers) subject to the GFSC purview risk-profile their clients taking into the consideration customer, product, country and interface risks. However, not all FIs (including banks) demonstrated that they understand that the firm's risk assessment should consider all relevant factors and not only the risk profiling of the customers, despite the requirement to make such assessments and document as part of the annual compliance report that FIs are required to complete, in line with the guidance set out in the GFSC's AMLGN.

341. In general, the banks have a good understanding of the overall ML risk faced by Gibraltar as an IFC and of the inherent vulnerabilities of certain factors. For example, banks understand well the risks related to eligible introducers (e.g. they stated that they would conduct their own CDD and do not rely on introducers' CDD); non-face-to-face on-boarding of clients and transactions; complex legal structures; and geographic risks. E-money providers, fund managers and administrators and *bureaux the change* have also a good understanding of the ML risks faced by Gibraltar. However, money lenders, MVTs and insurance sector understanding of risks is less satisfactory (both on threats and vulnerabilities).

342. The TF risk by FIs, in particularly by banks, e-money providers and MVTs is not properly understood, as it tends to focus only on sanction screening, without proper consideration of transactions to high risk countries. The GFSC study on high risk transactions has highlighted the absence of any TF related SARs submitted against the backdrop of over 30,000 transactions linked to high-risk countries.⁶⁵

343. In general, the FIs' understanding of the ML and FT risk is to some extent affected by the shortcomings noted in the analysis of IO.1 concerning the country's understanding of risk. The lack of an assessment of the banking sector's risks (at sector and product/services level) in the 2016 NRA, withheld from this important sector the country's perspective on the risk that this sector is facing, and of the specific threats and vulnerabilities affecting the sector, thereby affecting banks' capacity to conduct a risk assessment at the firm's level taking into account the sectoral risks as identified by the country.

344. As regards the understanding of AML/CFT obligations by FIs, as noted under 5.2.4 FIs, including banks, do not always understand their obligations in relation to BO requirements (e.g. BO is not always the shareholder holding more than 25% of the shares, but also the person having ultimate effective control over the customer). This is an issue particularly for banks who have corporate and trust clients, including introduced by TCSPs. Some of the FIs (e.g. money lenders and value for money transfer), did not exhibit a good understanding of their AML/CFT obligations. Except for some of the banks and DLT providers, awareness of the specific TFS obligations was not satisfactory.

DNFBPs

345. TCSPs and online gambling providers have, overall, a better understanding of the ML/FT risks that they are facing than other types of DNFBPs, particularly real estate agents (REAs). While the individual TCSPs met onsite were, with varying degrees, aware of the 2018 NRA findings, their association (consisting of TCSPs) was not, and did not fully appreciate the risk that this sector is facing. The AT noted, however, that one TCSP firm had transposed in its internal policies the risk classification of the 2018 NRA, considering only e-money as high risk and the rest of the other 12

⁶⁵ "Overall, Gibraltar banks have handled a total of GBP 136,473,110 from high risk countries and conflict countries (GBP 76,860,458 received, and GBP 59,612,653 issued). A high-level assessment of this industry would suggest that it has traditionally shown good level of awareness of the general FT related risks. However, the absence of any TF related SARs submitted against the backdrop of over 30,000 transactions linked to the high-risk countries (approximately 80,000 including the Drug transit/producing countries) could potentially raise some concern, and at the very least, warrants some further investigation."

higher risk sectors identified by the NRA as “medium to low” risk, which is not consistent with the findings of the 2018 NRA. With very few exceptions, REAs were also generally not knowledgeable of the findings of the 2018 NRA, which has classified real estate investments as 8th out of 13th higher risks and of the risk affecting the real estate sector. In the opinion of REAs, their profession is prevented from the abuse of ML since they are only acting as intermediaries between sellers and buyers, and not handling the clients’ funds. They do not take into account the fact that top buyers in the real estate sector are non-residents, which increases its inherent vulnerability to ML.

346. Of the DNFBPs interviewed the ones most cognizant of the requirement to assess the risk that the firm is facing were only online gambling providers, although one firm stated that they did their risk assessment considering the UK NRA and not Gibraltar’s. In general, the other DNFBPs seemed not always aware of the requirement to assess the firm’s ML and FT risk as a whole (including the risk posed by products and services and channels of distribution and of the customer’s base and not only in terms of risk profiling of the customers), particularly REAs. TCSPs and lawyers interviewed by the assessment team risk-profile their customers (TCSP consider customer, product, country and interface risks, as per the GFSC’s instructions).

347. Of all DNFBPs types, REAs have the least satisfactory awareness of AML/CFT requirements. Awareness of targeted financial sanctions (TFS) and their implication is generally not satisfactory by the DNFBPs, except for some of the TCSPs and online gambling providers which are part of a group.

5.2.2. Application of risk mitigating measures

348. REs are required to implement AML/CFT preventive measures to mitigate their ML/FT risks. However, the extent to which these preventive measures are adequately applied varies between and within sectors, as noted in the analysis below. With respect to FT, REs rely on sanctions screening tools to mitigate their FT risks. The detection and reporting of FT-related suspicious transactions, as also noted by the GFSC, is not adequate if compared with the number of transactions to/from conflict zones; many firms were not aware of their new legal requirements in implementing TFS, which were only introduced prior to the onsite visit.

FIs

349. FIs that fall under the purview of the GFSC (particularly e-money providers, fund managers and fund administrators, *bureaux de change*, money lenders and DLT) apply mitigating measures that are generally commensurate to their risks. In most cases these measures are the direct result of the thematic reviews recently undertaken by the GFSC (for example the one undertaken on e-money providers) and/or of the risk assessment undertaken by the firms. While these measures are informed by the assessment of the risk factors as required by the GFSC (customer, country, product and interface), some financial institution-types (such as banks), dealing primarily with high-net worth individuals (HNWI) or offering high risk services (e.g. private banking or pooled accounts) did not always demonstrate that they are taking measures that are commensurate to these specific risk factors. For example, in the case of lawyers’ bank accounts where the funds of their clients are pooled, one bank did not demonstrate to have specific risk measures, despite the firm’s being aware of the challenges arising from these types of accounts (e.g. bank’s full understanding of the BO of the pooled funds); while another bank has a specific regime in place for pooled accounts, consisting of specific checks and reviews by the relationship manager.

350. Data collected by the GFSC for 2017 and 2018 shows that the number of new customers not risk profiled by the institutions that fall under the purview of the GFSC has significantly decreased, from 121,415 (10% of all new customers) in 2017 to only 14 for the new customers onboarded in 2018. This is a positive trend, which shows that the risk profiling of the new customers onboarded

by the firms under the purview of the GFSC has significantly improved. However, the GFSC analysis of financial crime data for 2018 has evidenced that two banks had an excessively high number of customers that were not risk profiled and classified as “unknown”,⁶⁶ and that insurance managers had not reported data at all. While it is commendable that the GFSC has taken immediate actions to address these issues, it is of concern that in the case of one bank, the lack of risk classifications for this high number of customers was due to insufficient internal controls. These issues raise some concerns about the capacity of these FIs to apply risk-mitigating measures commensurate to their risk.

351. The AT has some reservations about FIs’ risk classification of their customers. In many cases the criteria used by the firms take into account the business activity or occupation of the customer and include several factors for the assessment of the geographic risk of the customer (e.g. not just the nationality, but also the residence or main place of business). However, it is not clear that risk elements related to the BO are factored in the analysis of the risk posed by customers, as evidenced by the internal policies, which are mostly focused on customer-related risk factors. For a jurisdiction like Gibraltar, where the vast majority of clients is non-resident, including BO factors in the risk classification of the customer would allow a more effective risk- segmentation and management of customers. Some FIs’ policies also refer to a default low-risk classification of customers that are in EU or EU-equivalent jurisdictions, which is not based on an actual assessment of the risk.

352. Banks and e-money providers’ implementation of TF-related suspicious transaction reporting measures are not commensurate with the TF risk that these sectors are facing, as evidenced by an analysis by the GFSC of 2017 transactions to/from conflict zones. The thematic review undertaken by the GFSC on e-money providers showed that all firms demonstrated a sound understanding of the ML/FT risks and most of them were proactive in mitigating and managing these risks. This was confirmed during the onsite visits with these firms. Of the other types of FIs, while *bureaux de change* demonstrated to have measures in place to mitigate their risk (e.g. limits to cash transactions, red flags for the detection of suspicious transactions) other types of FIs (e.g. insurance and money lenders) had less satisfactory (e.g. manual checks only for sanctions screening) or no measures in place.

DNFBPs

353. The level of application of risk mitigating measures by DNFBPs is uneven across sectors and DNFBP types. TCSPs, as well as online gambling providers, and to some extent, lawyers and dealers in high value goods apply mitigating measures that are commensurate to their risks. Online gambling providers have several measures in place to mitigate the risk of gambling frauds and ML/FT (e.g. no payment of winnings allowed to third-parties accounts or credit/debit cards; the winnings would always be returned to the same way of payment used), which were confirmed by onsite interviews.

354. The risk-mitigating measures identified by the country as a result of its NRAs and by the GFSC for particular sectors (for example those related to the use of power of attorney, or the requirement to ask and document systematically the tax rationale for the non-resident customer’s choice of Gibraltar, for the case of TCSPs) are generally well understood and implemented. Some of the policies reviewed by the AT provide caps or require approval by the compliance officer in case of cash receipt and distribution. However, REAs are not aware of the specific measures identified for their sector by the NRA (the need to have annual audited accounts).

⁶⁶ The two banks reported a total number of 602,589 as unknown, “given they do not hold the data or cannot extract the data”.

355. The thematic review conducted by the GFSC on TCSPs found that most firms applied a RBA on inception of a business relationship but not always when conducting periodic reviews. In addition, risk methodologies were found at times to not include the four key risk elements (i.e. Customer, Product, Interface and Country); when categorising a client under the four risk elements, several TCSPs do not consider risks posed by the nature of business of the client company or there is a lack of evidence that these factors are being considered. More in general, the thematic review of TCSPs showed that a significant number of firms could not evidence that policies and procedures are being applied effectively with some firms unable to evidence that all policies and procedures were adequately documented. The review highlighted also the use of unknown third-party entities or individuals providing nominee shareholdings, where there is lack of documented rationale, oversight and monitoring of the relationship, as an area of concern identified for various TCSP firms.

5.2.3. Application of CDD and record-keeping requirements

FIs

356. FIs demonstrated varying degrees of effectiveness in applying CDD requirements, whereby the record keeping requirements were generally well understood and implemented. However, the effectiveness of record keeping measures could be affected by the lack of an express requirement in the domestic framework to maintain records of BOs (the requirement is to maintain records on the “customer’s identity”). While the firms interviewed stated that they apply record keeping requirements concerning CDD measures for both customers and BO, it was not always clear in FIs’ internal policies that record keeping requirements apply also to BO. Basic CDD requirements (e.g. customer identification and verification) were generally well understood by all types of FIs. Insurance firms confirmed that they also apply CDD before paying out the proceed of a policy to a beneficiary.

357. The thematic review conducted by the GFSC on e-money providers showed that all firms conducted due diligence on the BOs of its corporate customers or programme manager. However onsite interviews showed that, the concept of BOs, as referring to the natural person having ultimate ownership and control of the customer, was not always properly understood by certain REs, particularly when complex ownership structures or trusts are involved. Several FIs, including some banks, insurance companies, some of the *bureaux de change* and money lenders focused only on identifying the 25% plus one ownership to be satisfied that they know who the BO is, and in few instances reference to these ownership percentages were made also in the case of trust customers. One bank had only very recently modified their internal policy to align the definition of the BO to the one envisaged by POCA (despite POCA being in place since 2016) and to include BO-verification requirements. Except for fund managers and administrators, not in all instances it was clearly demonstrated the firms’ awareness that BO, in the case of trusts, applies to the settlor, trustee, beneficiaries and protector. In the case of customers that are trusts, the challenges in identifying the BO are compounded by the AMLGN which, contrary to the standard, allow to consider the BO as the owner of 25% or more of the assets benefited from the trust. In general, the assessment team was left with the impression that there is not a comprehensive appreciation that the concept of BO includes also the case of a person having ultimate effective control on the customer, which may not necessarily be attained by owing a certain percentage of ownership rights.

358. Although the financial crime data collected by the GFSC for 2018 shows that the number of business relations to which simplified customer due diligence (SCDD) is applied has decreased since 2017, concluding that this is likely the result of a better understanding by the firms of the circumstances that trigger the application of SCDD, the 2019 thematic review of e-money firms showed that half of the firms were in breach of SCDD requirements as a result of their not having

updated their policies and procedures in line with the POCA. FIs with on-going business relations with their clients (such as banks and fund managers and administrators) apply periodic reviews of their customers files, based on the customer risk classifications and some trigger events; however, it is not clear that on-going monitoring of the business relationships and transactions is fully understood by all FIs. This is a challenge particularly for those firms that have legacy customers with asset holding vehicles that may not generate frequent transactions. The fact that some banks had not attributed a risk rating to many customers, impact these banks' effective implementation of on-going due diligence for those business relationships.

359. In the case of banks and e-money providers, on-going monitoring is generally automated with highlighted cases subject to proportionate review and tools to generate alerts and reports in respect of transactions or customers that may appear suspicious or unusual.

360. Application of CDD measures and reporting requirements by the firms that are licensed in Gibraltar but offer cross-border services (e.g. e-money and DLT/crypto currencies) could be affected by the absence of relevant clear guidance, particularly in scenarios that could trigger the applicability to other countries' AML frameworks (e.g. the stated residence of the customer, or its nationality or where the transaction is being performed based on the IP address). Several relevant REs met onsite were not always able to answer the questions on applicability of AML/CFT measures in complex cross-border scenarios (e.g. when customer is resident of another country or service provider server is located in another jurisdiction). The internal policy of one bank required the reporting of STRs related to Spanish residents both to the GFIU and the Spanish FIU.

361. REs met during the onsite confirmed that business is refused in case of incomplete CDD, but the examples provided referred mostly to the on-boarding of the client rather than to business relationship already established. Data provided by the GFSC for the entities under its purview (FIs) for the years 2016, 2017 and 2018 show that customers (and transactions) are declined or exited for financial crime reasons, or for failure to obtain satisfactory proof of identity (the data refers almost exclusively to banks and e-money providers), thus demonstrating awareness of these CDD obligations by these sectors. However, as noted under the analysis of STRs requirements, the FSA has also raised concerns, and the AT agrees, that the number of cases in which business was refused due to financial crime issues or because of tampered CDD data are not adequately producing also STRs to the FIU.

DNFBPs

362. DNFBPs demonstrated varying degrees of effectiveness in applying CDD requirements; whereby the record keeping requirements were generally well understood and implemented. However, as noted in the analysis of FIs, the effectiveness of record keeping measures is affected by the lack of a requirement in the domestic framework to maintain records of BOs. This could be particularly an issue for TCSPs managing complex corporate and trust structures.

363. TCSPs demonstrated, a good understanding of the concept of BO, as referring to the natural person having ultimate ownership and control of the customer. However, the thematic review of the sector completed by the GFSC in June 2018 evidenced of "Due diligence not conducted on the UBO or other individuals involved". For rest of DNFBPs, the general tendency observed by the team was to consider as BO only the person owning 25% plus one of the shares of a corporation. Except for TCSPs, the rest of DNFBPs not in all instances demonstrated awareness that BO, in the case of trusts, includes the settlor, trustee, beneficiaries and protector. As noted earlier the AMLGN provides that, in the case of trust, a beneficiary holding 25% or more of the assets within the trust can be deemed as BO, which is not in line with FATF.

364. DNFBPs with on-going business relationship with their clients, such as TCSPs online gambling providers and lawyers, apply periodic reviews of their customers files, based on the

customer risk classifications (in the case of TCSPs this is done according to the GFSC's guidance) and defined trigger events. The analysis of transactions to and conflict zones conducted by the GFSC highlighted that for TCSPs *"the threat/weakness may remain within the transaction monitoring systems and processes and understanding and documenting the economic activity of the entity under management. Experience gained from the many years of supervising this industry, particularly through client file testing at onsite inspection visits, tells us that there continues to be room for improvement in this area"*. The GFSC thematic review of TCSPs further indicated that a significant number of firms were not carrying out on-going monitoring in line with their own risk methodology i.e. client risk reviews are not completed when scheduled and that a number of firms have been unable to evidence on-going CDD, including where there is inactivity in the company and purpose for the client company is unclear.

365. In the case of online gambling operators, on-going monitoring is generally automated with highlighted cases subject to proportionate review (e.g. deposits/withdrawal history as well as gameplay monitoring) and tools to generate alerts and reports in respect of transactions or customers that may appear suspicious or unusual.

366. The OFT noted that many REAs failed to implement written AML/CFT policies and create procedures to appropriately record transactions, collect CDD documents or carry out risk assessments as required under POCA and by the OFT's Guidance Notes. Additionally, the collection of documents was often carried out mechanically and risk assessments were carried out as a mental process rather than a recorded one. There were also no differences between the levels of CDD collected for high risk and low risk clients.

367. TCSPs demonstrated that business is refused in the case of incomplete CDD, but the examples provided referred mostly to the on-boarding of the client rather for business relationship already established. See relevant reference under FIs for the years 2016, 2017 and 2018, mentioned under the FIs analysis, which applies also to TCSPs. Other types of DNFBPs were generally aware of their obligations triggered by failure to satisfactorily complete CDD.

5.2.4. Application of EDD measures

PEPs - FIs

368. FIs were in general aware of the definition of PEPs, of the applicability of enhanced customer due diligence (ECDD) measures to family members and close associates and had arrangements in place for the approval of the business relationship (or the continuation of an established business relationship) by senior management or special committees. However, not all FIs demonstrated a good understanding and/or implementation of requirements concerning the verification of the source of wealth and source of funds. The majority of the FIs interviewed were aware of the requirement to establish the source of funds, but there were few cases in which FIs (some banks and insurance companies and e-money providers) did not demonstrate awareness of the separate requirement to establish the source of wealth and funds. This could also be the result of the approach taken by the GFSC in its inspections. For example, in the thematic review of the e-money, the GFSC, when it comes to its expectations regarding the implementation by e-money firms of this particular requirement describes it as *"Assess and verify a PEP's Source of Funds and/or Wealth"*. In general, the AT noted a tendency to over-rely on information provided by the customer or (particularly for banks) certified by lawyers or auditors in verifying the source of wealth and the source of funds, including for high-net worth clients.

369. Through the Financial Crime Return, the GFSC obtains information on the number of clients classified as PEP, family member of a PEP or close associate of a PEP; and the information is required to be provided per country.

Table 28: PEPs

	Low	Med/Low	Med/High	High
Active individual customers classified as PEP	124	79	99	83
Active individual customers identified as a family member of a PEP	32	18	16	2
Active individual customers identified as a close associate of a PEP	23	24	28	11
Active individual customers profiled as high risk	1327	4291	1457	168

PEPs (DNFBPs)

370. DNFBPs are aware of the definition of PEPs (with the exception of some DNFBP types, particularly some real estate agents, who made reference to list of PEPs issues by FATF and Gibraltar), of the applicability of ECDD to family members and close associates, and had arrangements in place for the approval of the business relationship (or the continuation of an established business relationship) by senior management. However, not all DNFBP types that have stated to have PEP customers (TCSPs and lawyers) demonstrated a good understanding and/or implementation of requirements concerning the verification of the source of wealth and source of funds. The majority of the firms interviewed were aware of the requirement to establish the source of funds, but not always of the separate requirement to establish the source of wealth. There is a tendency to over-rely on information provided by the customer (e.g. bank statements) or (particularly for TCSPs and lawyers) certified by lawyers or auditors in verifying the source of wealth and the source of funds, including for high-net worth clients. For TCSPs the thematic review conducted by the GFSC noted that “*some firms did not conduct adequate CDD relative to source of wealth and particularly source of funds, to a level of plausible verifiability*” and that “*ECDD is not being applied as per the requirements e.g. in some cases PEPs are not being classified as high-risk relationships*”.

Correspondent Banking

371. None of the banks established in Gibraltar provide correspondent banking, though they do use correspondent banking for their business. These relationships are generally established at authorisation stage, and therefore get scrutinised during the application process, and they would entail an assessment of the risk associated in the establishment of the business relationship with the correspondent bank. If a bank intends to change correspondent banking relationship, this would mean a change in business plan and would require notification and approval by the GFSC. Banks were generally aware that they are not permitted to establish correspondent banking arrangements with shell banks, pursuant to domestic requirements in POCA. The GFSC requests annually information from banks on their correspondent banking relationships through the Financial Crime Return. Banks are obliged to advise through the Financial Crime Return where the correspondent banks are based. Data provided by the GFSC for 2018 shows that most correspondent banking relationships are established with institutions based in jurisdictions where the risk is low or medium low (however see the reservations the AT has expressed regarding the classification of the geographic risk utilized by the GFSC). Other FIs do not maintain correspondent relationships with foreign FIs. The AT has reservations about the exemption from the application of correspondent banking-related requirements applied by default, without an actual risk assessment, in the case of a FI from an EEA state (see analysis of R13).

New technologies (FIs and DNFBPs)

372. Banks, and e-money providers stated that they undertake a ML/TF risk assessment for all new products and services, as part of the GFSC licensing process and in the context of their risk assessment (the GFSC template for the risk assessment of the entities that fall under its purview specifically include also non-face to face). DLT providers showed also good awareness of the ML/TF risks associated to new technologies and measures in place to mitigate them. The GFSC has noted that with the implementation of regulatory framework for new business activities such as DLT providers, these firms take on new technologies as part of its systems of controls for CDD and on-going monitoring. Examples of these include collecting PC signatures and IP addresses from clients; IP and keyboard languages recorded and compared to physical billing and shipping addresses, and further out-house technology checks are conducted through external service providers such as World Check or C6 Intelligence.

373. Data on new customers on-boarded in 2017 and 2018 by the firms under the purview of the GFSC shows that the overwhelming majority new clients are on-boarded non-face-to-face (96% of new clients in 2017 and 89% of new clients in 2018). However, the 2019 thematic review of e-money firms showed that half of the firms were in breach of SDD requirements, given they had not updated their policies and procedures in line with the POCA. This raises serious concerns about the e-money sector application of simplified CDD to clients that may have been on-boarded non-face-to-face, considering that the majority of new clients reported for 2017 and 2018 belong to e-money providers (in 2017, out of a total of 1.169.400 customers of all firms under the purview of the GFSC, 776.971 belong to e-money providers; in 2018, out of a total of 1.386.404, customers of all firms under the purview of the GFSC, 968.531 belong to e-money providers). Data of 2018 shows also that, in the case of insurance, 100% of the new clients in 2018 was on-boarded non-face-to-face, however the insurance firms interviewed did not show sufficient awareness of the risk posed by new technologies. Among DNFBPs that use new technologies, online gambling providers exhibited a good understanding of the risk and vulnerabilities related to the use of such technologies and provided examples of measures required by their policies to mitigate the risk, both related to prevent the risks of frauds as well as ML/FT.

Wire transfers

374. Banks and MVTs provide wire transfers services. All transfers below EUR 1,000 are required to be accompanied by the required originator and beneficiary information (Art.5(2) and 6(2)), WTR). The AMLGN addresses the obligation of the payment service provider to verify the information on the payer only when the amount exceeds 1.000 euro. Gibraltar does not apply the minimum threshold. The compliance report, that the GFSC shares with the firms under its purview for them to conduct a self-assessment, includes specific provisions and guidance for the implementation of wire transfers-related requirements. MVTs interviewed by the AT belong to large international firms that apply group-policy requirements, including in the implementation of wire transfers. These firms, as well as banks have software that would not allow or block the execution of wire transfers if the all information required is incomplete or if there are hits with internal lists (e.g. sanctions-related lists embedded in the software). MVTS have cases where the systems have blocked wire transfers because they were related to high-risk types of customers (e.g. PEPs) although they also mentioned that in some cases the transactions would be blocked without specific indications of the cause from the software (which is not ideal, as the information would have to be specifically requested from the group compliance officer, which may affect the timeliness of certain processes – e.g. if they had to notify the GFIU about a true match with a UN list).

Targeted financial sanctions related to FT (FIs)

375. The understanding of TFS and their operational implications needs considerable improvement across all sectors, particularly the smaller FIs. Most types of FIs (banks, fund managers and funds administrators, e-money providers, DLT providers and bureaux de change) are doing checks of customers at on-boarding and periodically (several FIs using commercial databases), but it was not clear to all that the checks should be done also on BOs and senior management in case of corporate entities. The issues noted in the analysis about the FI's understanding of BOs also affects the implementation of TFS, as it hinders the identification of potential targets that are BOs of the client. FIs providing wire transfers (banks, e-money providers and MVTs) screen also the beneficiary of the transactions. The review of some of the FIs' policies confirm that there is considerable room for improvement: it is not always clear that TFS are broader than freezing of funds, and in one case (a bank) the policy required only the blocking of transactions only, but not the freezing of the entire account).

376. There was a mixed understanding on which "list" to screen against, some FIs referring to OFAC, FATF, and some small FIs (e.g. money lenders, MVTs) not being aware of the existence of lists; some firms referred to the list of countries under sanctions confusing them with list of persons/entities lists. For the e-money sector, the GFSC analysis of transactions to/from conflict zones evidenced that "*not all firms included EU sanctions lists in their screening procedures*". There was insufficient awareness of internal procedures for dealing with matches (potential or real) across all types of FIs as well as on the legal requirements and implications concerning TFS, in particular those stemming from the recently introduced Sanctions Act, although firms were conducting sanction screening prior to that.

Targeted financial sanctions related to FT (DNFBPs)

377. The understanding of TFS requirements needs significant improvement also across all types of DNFBPs. DNFBPs interviewed by the AT stated that they did checks of customers at on-boarding and periodically (TCSPs and online gambling providers also using commercial databases), but it was not clear to all that the checks should be done also on BOs and senior management in case of corporate entities. As in the case of FIs, there was a mixed understanding on which "list" to screen against, some referring to OFAC, FATF, and some real estate agents not being aware of the existence of lists. Except for some law firms and some TCSPs interviewed by the AT there was insufficient awareness of internal procedures for dealing with matches (including with false positives). As in the case of FIs, knowledge on the new legal requirements introduced by the Sanctions Act and implications concerning TFS was insufficient. The issues noted regarding the DNFBPs' understanding of BO also present a hindrance to the identification of potential targets, thus affecting the implementation of TFS.

Higher risk countries (FIs and DNFBPs)

378. FIs (particularly banks, DLT providers and e-money providers), had overall a good understanding of jurisdictional risks, including the case of higher risk countries identified by FATF and of the ECDD measures to be taken in the case of customers or FIs with links to such countries. Firms would either check regularly the FATF websites or, for those that are part of international groups, receive alerts from the group compliance officer. The GFSC has instructed the firms under its purview to classify as "high-risk" clients with links (e.g. nationality or residence) to countries identified by FATF as posing a higher risk, and this requirement was generally well understood, except in the case of some small FIs (e.g. money lenders), that were not always aware of the existence of higher risk countries identified by FATF. However, some firms would consider by default as low risk customers or FI from EEA countries, which is not based on actual risk.

379. DNFBPs had a fair understanding of jurisdictional risks, including the case of higher risk countries identified by FATF (particularly TCSPs, online gambling providers and some of the lawyers interviewed, but few real estate agents).

5.2.5. Reporting obligations and tipping off

FIs/DNFBPs

380. The charts below show the breakdown of STRs by industry sector and underlying predicate offences indicated by the suspicion for 2017 and the first six months of 2018.

Table 29: STRs submitted by industry and predicate offence (2017)

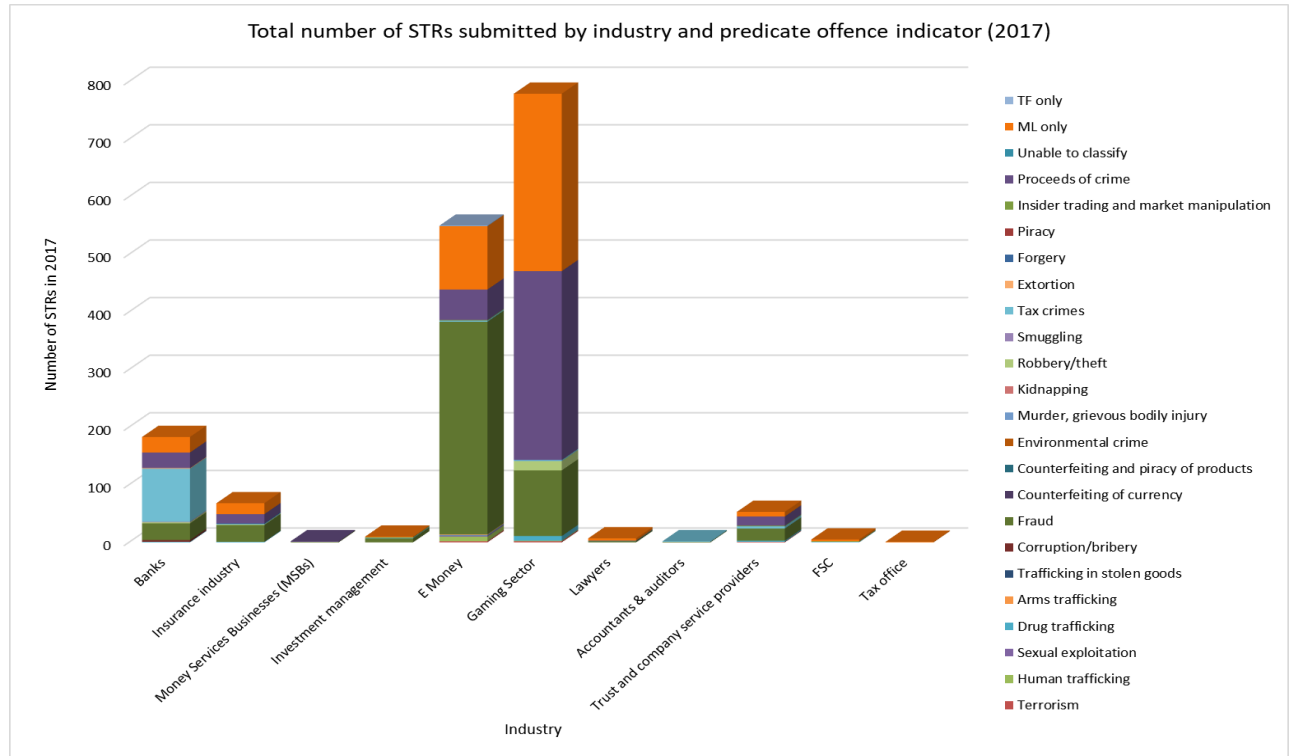
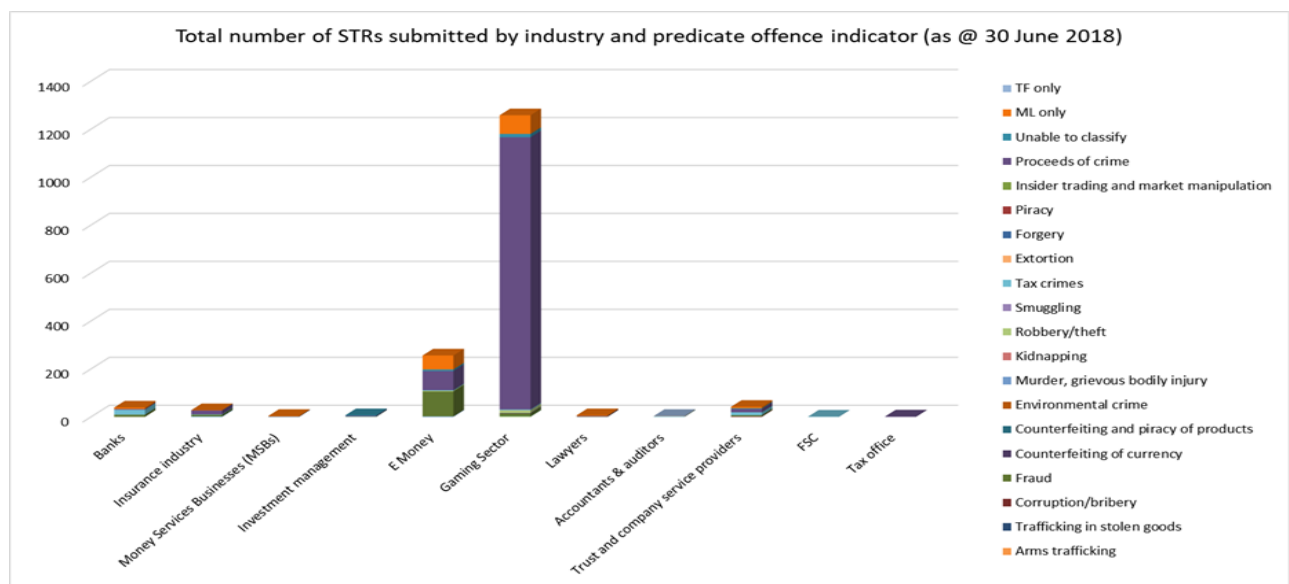


Table 30: STRs submitted by industry and predicate offence (as of June 2018)



FIs

381. FIs interviewed by the AT demonstrated overall a very good understanding of the STRs legal requirements and of tipping off measures. The practical measures to prevent tipping off are included by licensed entities in any on-going AML/CFT training to promote an understanding and an awareness of what would constitute a tipping-off offence. This is reviewed by the GFSC as part of its risk assessment of the firm. The FIs policies reviewed by the AT have detailed provisions on tipping-off. However, one of the banks interviewed could not elaborate on their procedures to prevent tipping off the clients.

382. Despite the good understanding demonstrated by the FIs interviewed of their legal requirements, the AT has reservations about REs effective implementation of STR-related requirements. As noted under IO.6, there were a number of cases in which, in the opinion of LEAs, STRs may have been filed by a firm only after the firm became aware (e.g. through media) of an on-going investigation. The cases in which an STR disseminated by the GFIU to LEA referred to an on-going investigations account to the majority of STRs disseminated to LEAs. This “reactive” form of reporting is of concern.

383. As it can be observed from the table below, extracted from the GFSC analysis of financial crime data for 2018 for the entities under the purview of the GFSC, the number of STRs is not commensurate with instances in which clients were exited or transactions declined on financial crime concerns. In particular, the GFSC noted that *“the total number of reports made to the GFIU and/or other law enforcement agency is relatively low, compared to the number of false or tampered documented detected/suspected (see above). These should have been reported to the RGP and/or the FIU”*. The AT shares the GFSC’s concerns.

Table 31: GFSC data of financial crime 2018

Number of clients (not yet onboarded) declined for suspected financial crime reasons	8,095
Number of clients exited (with whom the firm holds a business relationship) for suspected financial crime reasons	1,468
Number of clients where false or tampered documents were detected or suspected when verifying the authenticity of KYC documents	2,381
Number of transactions declined for suspected financial crime reasons	3,643
Number of reports made to GFIU and/or law enforcement with respect to detected or suspected false or tampered	57
Number of suspicious activity reports submitted to the GFIU	645
Number of disclosures made to the GFIU resulting in declined or exited business relationships	1,513

384. The GFSC conducted also an analysis of transactions to/from conflict zones, which showed that the near absence of TF-related STRs is not commensurate to the TF risk that banks, e-money providers and TCSPs are facing. In particular, the GFSC noted that there was only one TF related SAR submitted in 2017 by a e-money firm, which is *“somewhat at odds with the disproportionate number of transactions linked to high-risk countries executed through E-money firms”*. In the case of banks the GFSC noted that *“the absence of any TF related SARs submitted against the backdrop of over 30,000 transactions linked to the high risk countries (approximately 80,000 including the Drug transit/producing countries) could potentially raise some concern, and at the very least, warrants some further investigation”*. During the thematic review of e-money the GFSC identified breaches that had not been notified to the GFSC, with some not having been addressed in a timely manner.

385. More in general, given the low number of disseminations by the FIU and the near absence of investigations triggered by STRs, questions can be raised about the quality of the STRs and the fact that the reported STRs do not appear to be commensurate to the threat that Gibraltar is facing, particularly the cross-border ML threat. This is particularly an issue for of the banks, given the ratio between STRs submitted to the FIU and disseminated to law enforcement, and for e-money providers, whose number of STRs is excessively high and, as noted under the analysis of IO6, is an indication of defensive reporting.

386. The scope of the reporting requirement as envisaged in the legislation might also affect the effectiveness of the reporting regime, in particular the specific suspicion required for reporting and the lack of a clear requirement to report attempted transaction (the requirement is to report attempted ML) – only 4 were reported to the authorities, which is not commensurate to the risk of ML/FT that the jurisdiction is facing.

387. AT was also was given inconsistent answers to the issue of the FIU's power to request additional information (either following up to an STR or for the purpose of conducting financial analysis), as most firms stated that a production order is needed, when it is not.

DNFBPs

388. As regards DNFBPs, in addition to issues noted earlier in the case of FIs (which are also relevant for DNFBPs), TCSPs and lawyers exhibited a good understanding of the reporting requirements, except for the legal framework concerning the provision of additional information to the GFIU, which was poorly understood: the majority of DNFBPs interviewed stated that they would need a production order in order to provide any additional information or document to the GFIU. The understanding of other DNFBP types, particularly the procedures for reporting to the GFIU through the new platform, was not always satisfactory.

389. Quality issues of the STRs submitted can be raised, given the low number of disseminations by the GFIU and the near absence of investigations triggered by STRs, also for DNFBPs. This is particularly an issue for the online gambling operators, given the materiality and risk of the sector, where there is a clear tendency of defensive reporting, as noted under the analysis of IO.6. Authorities explained that this defensive reporting is also due to the position of a foreign regulator, which has deemed that the refusal to submit copies of personal finance documents if the customer's losses exceed their 'visible lifestyle' must trigger a SAR and closure of the account. This unresolved issue resulted in a near tenfold increase in the number of SARs in 2018 associated with that state. A significant issue is also the dual reporting regime (to the FIU and the GCC) still existing in the gambling sector, which had not been fully resolved at the time of the on-site (an analysis of internal procedures of some of the online gambling operators still showed the GCC as the primary recipient of the STRs; the GCC has a platform for following up on reported suspicious transactions). It is noted that one online gambling operator stated that they would report to the GFIU and also to the FIU of other countries where they have "agreements" to file SARs. This confirms the issue, noted earlier, of a lack of a clear guidance on which legal requirements to apply in the case of firms licensed in Gibraltar but passporting in other countries and having a multi-national dimension.

5.2.6. Internal controls and legal/regulatory requirements impending implementation

FIs

390. In general, FIs interviewed by the team demonstrated to have good internal controls and procedures to comply with AML/CFT requirements, particularly those that are part of a group, commensurate to their size and risks, including internal audit requirements. The GFSC-developed self-assessment questionnaire for the firms under its purview specifically includes an independent audit function, and risk-sensitive policies, controls and procedures. However for those FIs,

particularly banks, and e-money providers) part of larger group the seniority of the money laundering compliance officer (MLRO) seemed not appropriate and the reporting lines were too convoluted, without a clear and direct reporting line by the MLRO to senior management of the firm, but, rather, to or through the compliance officer, either at group level or through other lines. For example, the policy of one bank provided that the MLRO can have a “reasonable” access to information. In several of these cases the operational monitoring of compliance was outsourced to firms operating from outside Gibraltar, as confirmed also by the 2018 data on the firms under the purview of the GFSC, which shows that 36% of such firms outsource their systems of controls or compliance measure, in full or partially, with respect to AML/CFT requirements. While outsourcing compliance arrangements may be justifiable in the case of small FIs, the cases in which such arrangements are outsourced in Gibraltar include also large FIs such as banks, insurance companies and e-money providers. Outsourcing compliance by these types of firms could result in a detachment of the compliance functions from the core operational businesses of the FIs and may affect the effectiveness of the compliance arrangements of these firms.

391. There are no FI secrecy laws or application of common law in Gibraltar that inhibit the implementation of AML/CFT measures or that restrict the exchange of information between firms.

DNFBPs

392. DNFBPs have (in varying degrees) internal controls and procedures to comply with AML/CFT requirements, commensurate to their size and risks. However, there were instances (large firms providing online gambling and TCSPs) in which the ML compliance officer (MLRO)’s position within the firm was not at management level or seemed not appropriate or commensurate to the size of the firms, including for a lack of a direct reporting line to the firm’s senior management. TCSPs and lawyers were particularly sensitive to the confidentiality of the information they hold on their clients. They also were, among the REs, interviewed, the least aware (or showed excessive caution) of the newest requirements that entitle the GFIU to obtain additional information from REs without a court order, stating that they would feel more comfortable in sharing information on their clients with the GFIU if requested with a court order.

Overall conclusions on IO.4

393. **Gibraltar is rated as having a moderate level of effectiveness for IO.4.**

6. SUPERVISION

Key Findings

Immediate Outcome 3

- a) All supervisory authorities apply licencing/registration and screening measures to prevent criminals and their associates from abusing FIs and DNFBPs. However, they target only new applications and not already licenced individuals. Although legal requirements do not extend to checking BOs and their source of funds, and there is no legal requirement to reject applicants with criminal background relevant for fit and proper, this is generally done in practice.
- b) The GFSC and GGC have a robust understanding of their sectoral ML/FT risks. The OFT risk understanding is in its nascent stage, although it is developing fast. The other supervisors have an insufficient understanding of ML/FT risks.
- c) The GFSC and OFT have developed documented procedures for risk-scoring all supervised entities. At the time of the onsite other authorities either had not yet developed clear methodologies for assessing the supervised entities' ML/FT risks or had not categorized them.
- d) The GFSC uses primarily Thematic Reviews for AML/CFT supervision. At the time of the onsite such reviews have been completed for the TCSPs and e-money sectors. Supervision for the rest of the FIs and DNFBPs that are licensed by the GFSC is either triggered by events or is based on the general risk score that includes, but does not focus on, financial crime risk. The number of inspections based on this latter approach, compared with the thematic reviews, is low.
- e) On-site supervisory plans in the gambling sector are based primarily on the size of the REs (as this is considered commensurate with the risk they pose by the supervisor), and up until the end of 2018 they were also based on the number of SARs transmitted. No violations were recorded.
- f) The RSC has only recently been appointed with AML/CFT supervisory responsibilities and has mainly focused on gathering information on supervised entities and raising their awareness of AML/CFT obligations.
- g) The number of sanctions applied to both FIs and DNFBPs is low. Authorities consider that measures applied so far (remedial plans) are effective and proportionate taking into account the breaches identified, and would consider applying other sanctions (fines, revoking the licence) only in case of more serious breaches.
- h) Accountants and tax advisors have not been subject to any AML/CFT inspections because dedicated supervisors for these types of REs have not yet been appointed.⁶⁷
- i) The authorities could not fully demonstrate a proportionate and dissuasive approach to sanctioning for breaches of AML/CFT requirements.
- j) Overall, there seems to be good communication between REs and supervisors on AML/CFT matters through open and direct communication, facilitated by the small size of the jurisdiction, with the exception of requirements related to TFS, where there is a need to reach out more to REs.

⁶⁷ In practice, the Financial Secretary, who is the accountants and tax advisor's supervisor, does not perform any supervisory activity in AML/CFT matters.

Recommended Actions

General

- a) Address the deficiencies identified in Technical Compliance Annex under R.26.
- b) Engage with accountants and tax advisors. Even if there is no dedicated supervisory authority appointed for them, the Financial Secretary should at least conduct a discovery and awareness raising exercise for this sector.
- c) All authorities, and in particular the GFSC and the GGC, should re-evaluate the proportionality test used in analysing the AML/CFT breaches and penalise such in a more dissuasive manner. The publication of such penalties (where necessary preserving the anonymity of those in breach) should be considered.
- d) All authorities would benefit from improving their statistics on outcomes of supervisory activities and other regulatory actions.

GFSC

- a) The GFSC could benefit from periodic discovery exercises to identify those individuals in notifiable positions that were authorised in the past and have not undergone any on-going due diligence in recent years. The GFSC should ensure that they have remained fit and proper, particularly in respect of any involvement or association with criminal activity. This discovery exercise could also reveal any non-compliance with the requirement to notify the authority about any changes which had occurred.
- b) The GFSC could take advantage of the recent experience of growing pending cases in the authorization process and reconsider its overall approach to avoid similar situations, should those re-occur. This could include a more structured approach, including putting more emphasis on the application stages.⁶⁸
- c) In relation to unauthorized activity, the GFSC should be more proactive and have in place more specific tools to discover unregulated entities that offer (or advertise) services.
- d) The GFSC should document the discussions and meetings on risks and undertake formal risk assessments of the sectors, particularly those that, as a result of these discussions, appear to be of a higher risk. The GFSC should also update the general Risk Framework to include the role of the new AML/CFT team.
- e) The GFSC should continue to add to and improve the metrics of the Risk Based Methodology to enhance and refine the understanding of an individual level of risk and in relation to the general risk framework, the GFSC could consider finalising the development of metrics as initially intended.
- f) The GFSC should continue to issue guidance on regulatory expectations and maintain an appropriate awareness level of AML/CFT requirements among REs.
- g) The GFSC should finalise the discovery exercise for MVTs and take relevant follow up actions.
- h) The GFSC should ensure that the AML/CFT supervisory calendar is respected and all Thematic Reviews are finalised within the timeframe indicated therein.

⁶⁸ In order to eliminate from the start any clearly un-fit candidates due to evident inadequacy (e.g. lack of required experience) to avoid engaging more resources in their examination.

GGC

- a) The GGC could benefit from developing manuals to assist staff in the process of authorising and licencing entities and individuals.
- b) The GGC should undertake documented risk assessments of the sectors it supervises (in addition to providing input to the NRA) and update them on an on-going basis. The supervisory focus could be improved if the GGC would continue to enhance and document the methodology for assessing each entity's ML/FT risk and adopt a clear supervisory policy based on the level of risk returned by this.
- c) The GGC should continue to engage with the industry by providing training sessions on new developments in the AML/CFT field and on the requirements of the POCA, especially concerning STR reporting.

OFT

- a) The OFT could update the business licence application manual to make it clearer that the fit and proper requirements apply to all applicants and not only to the newly established REA of an HDV (or for senior managers or BOs of only newly established HDV or REAs) or those subject to transfer of business.
- b) The OFT should update the annual report form to make it clearer that it is only financial audited data which may be submitted 9 months after the end of the year but the rest of the data needs to be provided in a timely manner.
- c) The OFT should ensure that any newly appointed senior manager or controller is notified to, and subsequently checked by the OFT immediately, instead of on an annual basis through the annual report form.
- d) The OFT should continue to develop the internal manual on on-going monitoring, in particular develop the risk score methodology so that it would 'assist the officers in executing their role as regulators on an RBA system'⁶⁹ in practice.

RSC

- a) The RSC could benefit from developing the formal policy for licensing in its coverage of AML/CFT issues and so that it clarifies when criminal records should be provided.
- b) The RSC should engage on an on-going basis with the industry to identify any new solicitors or barristers who have begun to offer services covered by the POCA.
- c) The RSC should formally assess the risk of the sector, develop the relevant methodology to evaluate the ML/FT risks posed by each entity and determine an on-site inspection cycle based on the results.
- d) The RSC could collect information from the RE (e.g. sending out periodical questionnaires) for conducting its risk assessments.
- e) The RSC should move from introductory visits to providing training sessions regarding new AML/CFT developments, including any new requirements under the POCA.

⁶⁹ The methodology states that it 'assist the officers in executing their role as regulators on an RBA system'.

394. The relevant Immediate Outcome considered and assessed in this chapter is IO.3. The Recommendations relevant for the assessment of effectiveness under this section are R.14, R. 26-28, R.34, and R.35.

6.1. Immediate Outcome 3 (Supervision)

395. All FIs and DNFBPs are regulated and supervised in Gibraltar. The GFSC supervises all FIs, TSCPs, DLTs, auditors and insolvency practitioners, while the GGC, RCS and OFT supervise other DNFBPs (see Chapter 1).

396. Positive and negative aspects of Gibraltar's supervisory regime were weighted similarly to IO.4. In practice, the Financial Secretary, who is the supervisor for accountants and tax advisors, does not perform any supervisory activity in AML/CFT matters. Given the fact that they only perform book-keeping activities, this does not affect the effectiveness of AML/CFT supervision overall.

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

397. All supervisors apply a number of controls to prevent criminals and their associates from entering the market. The type of information checked, and the extent of the verification varies amongst the different supervisors. For already licensed individuals, there are no specific procedures in place to periodically re-apply due diligence measures. Thus, it is not ensured in all instances that criminals and associates are prevented from holding/being the BO or performing a management function respectively in FIs and DNFBPs.

398. In relation to unauthorised activity, those cases that were brought to the attention of the supervisors have been addressed, but not all authorities have detailed procedures or mechanisms in place to detect unlicensed activity.

GFSC -FIs, TCSPs, DLTs, auditors and insolvency practitioners

399. As part of its authorisation process the GFSC applies a number of controls to prevent criminals and their associates from owning or controlling FIs and DNFBPs supervised by the GFSC. Screening measures to prevent criminals from engaging with the market consist of making inquiries to determine whether an applicant has a criminal record. Criminal records are obtained, and the applicant is required to declare on a questionnaire about any investigations (both criminal and administrative), convictions and sanctions. Although the legal framework does not explicitly prohibit persons with criminal records from holding positions of significant influence (see Technical Compliance Annex C.26.3) in 2016 the GFSC published a Policy Statement on its website, which set out its presumption that any individual convicted of an offence involving dishonesty, fraud, financial crime a ML offence, or who has been subject to matters relating to those offences, would not meet the fit and proper requirements.

400. In 2017, the GFSC adopted a new Due Diligence Methodology, which required mandatory checks of criminal records for all individuals relevant to the application: board members, shareholders and controllers in excess of 10% controlling rights,⁷⁰ compliance officers/MLROs and associates of key individuals in cases where those are identified. Fitness and properness measures were also applied prior to 2017, these included criminal record checks and vetting with the RGP. The new and former Due Diligence Methodologies were presented to the AT with examples of where due diligence was performed on all controllers considering the risks posed.

⁷⁰ Although in practice the GFSC has showed that this includes BO as defined by FATF, it does not clearly mention this in the Due Diligence Methodology (see comments under TCA C.26.3)

401. The GFSC checks relevant databases (e.g. the Shared Intelligence Service database operated by UK’s FCA⁷¹, Companies’ House Register and commercial databases), and open sources and requests/receives information from domestic authorities, such as the RGP and the GFIU. In addition, the GFSC sends requests to relevant foreign authorities (e.g. Ireland, Malta, Bermuda, Dubai and Portugal and specifically with the FCA and the PRA in the UK). Each individual related to the application is additionally checked against sanctions lists, including UN TFS lists, and checks are performed again each time new names are added to the lists.

402. The AT was provided with a list of cases illustrating the effectiveness of applying these measures in preventing criminals, including their associates, from entering the market.

403. Any change of controllers or managers and directors has to be notified to the GFSC and each person undergoes the same Due Diligence scrutiny. For already licensed individuals, there are no specific procedures in place to periodically re-apply due diligence measures. Re-application of due diligence is applied only in case of trigger events (e.g. receiving adverse information) and some simplified checks on governance adequacy are applied as part of the supervisory duties.

404. The number of applications in the last 3 years has been increasing. According to the authorities this is due to the fact that 3 new sectors had to be covered when new regulations for DLT providers, pensions and foundations came into force.

Table 32: Number of applications received in the last 3 years and settled upon the powers given by the SBPR:

	2016		2017		2018	
	Individuals	Licensees	Individuals	Licensees	Individuals	Licensees
Received	272	52	356	129	498	129
Approved	247	34	280	81	165	45
Withdrawn	27	15	49	12	29	2
Rejected	2	0	0	0	0	0
Pending	0	3	27	36	304	82

405. The GFSC has very rarely formally rejected applications⁷². That said, many withdrew their applications during the authorisation process because of advice given by the GFSC (90% of withdrawals were for lack of experience) or because of a higher level of scrutiny applied by the GFSC. The GFSC indicated that where adverse findings arise, a higher level of scrutiny is always applied and in most cases an applicant becomes discouraged from pursuing a licence application and withdraws. The AT was provided with a list of cases illustrating effectiveness in this area. Although such an approach might be adopted as a precaution, it can also tip-off potential candidates who would be rejected for not being fit-and-proper. Any applicant can try to get accepted and then withdraw with no risk of rejection and no consequential risk of reputational damage. This creates in the view of AT the risk that some less fit or proper individuals could eventually be approved.

406. The GFSC has 2 Authorisation Teams, each amounting to approximately 11 people and one of them specifically dedicated to DLT providers. In cases of more complex structures and larger entities, such as banks, the GFSC has used external consultants by obtaining reports from a well-known auditing firm and has performed on-site pre-authorisation visits to premises held abroad. The GFSC provided some examples of bank authorisations to the AT. The structures were complex, with multiple layers and with different entities (such as private companies or trusts) incorporated

⁷¹ This is a mechanism for UK regulatory bodies to collect and share material on individuals and firms. FSC is a member of this mechanism

⁷² The FSC rejected 2 applications in 2016.

or established in overseas jurisdictions, making the identification of BOs more challenging. The AT was provided with a list of cases illustrating the effectiveness of applied controls.

407. In relation to unauthorised activity, there is no written procedure in place to identify unlicensed entities. However, the GFSC takes into consideration any relevant information (e.g. gathered through periodic online searches of the company register or for advertisements, re-checking management positions or BOs) to investigate further. 19 unlicensed entities have been discovered since 2015. Most were companies that falsely declared on their websites that they were registered and supervised in Gibraltar. Additionally, some measures have been applied to identify unlicensed TCSPs (e.g. Companies House Register shares information on individuals who are registered as a manager/administrator/shareholder in a significant number of companies).

408. Auditors and insolvency practitioners are licensed by the GFSC and undergo the same due diligence checks as every other notifiable individual. They are also checked by different self-regulatory bodies from the UK jointly with the GFSC. Their activity is limited, posing a low risk of ML/FT.

409. In relation to MVTs agents, the GFSC is undergoing a discovery exercise to ensure that it holds current and accurate data.

Virtual Assets

410. Gibraltar is one of the few jurisdictions that have a regulated DLT providers' sector since 2017⁷³ with the first licenses granted in 2018. A dedicated DLT authorisation team, with a size comparable to that of the general authorization team, has been put in place. It applies the same fit-and-proper measures and general procedures as for the other FIs.

411. The licencing procedure takes from a few months to over a year and includes checks of internal AML/CFT procedures and controls and a risk assessment of the products offered together with checks on individuals, including interviewing and searching for any criminal records. Once a firm is licensed, the GFSC would perform a follow-up onsite inspection to ensure that these procedures are in place. Such approach was confirmed by the firms interviewed onsite.

Other DNFBPs:

GGC

412. The licensing authority for the gambling sector (casino and online gambling) is the Minister for Gambling, with the assistance of the Gambling Commissioner (GGC) and Gambling Division (GD).

413. The GGC applies fit-and-proper checks to business-to-business (B2B) and business-to-customer (B2C) applicants and some checks for suppliers of licensed operators (e.g. checking directors and shareholders of over 5% holding and the contracts between the parties).

414. The GGC's licence application procedure involves a 2-stage process (pre-application and application). In most cases applicants use the assistance of lawyers or TCSPs. No matter if such assistance is used or not, the GGC's licence application procedure and checks are the same. The application form requires the disclosure (among other general requirements) of all parties' *'corporate or otherwise, that are involved in the beneficial ownership or legal control'* with more than a 10% interest or shareholding. It is not publicly available and is provided only to those applicants who pass the initial pre-application process.

415. In 2018, a total number of 10 applicants were rejected at the pre-application stage (e.g. for insufficient transparency of the applicant), with several others having been rejected in previous

⁷³ Financial Services (Distributed Ledger Technology Providers) Regulations 2017

years. For the period 2014-2018, the AT was presented with a total number of 5 denied applications from operators who had been licensed already in other jurisdictions. The rejection was based either on *'questionable or even dubious licensed business models'* or for not demonstrating full transparency of ownership and controlling interests. The GGC has provided a list of case examples to establish effectiveness in this matter.

416. The GGC does not have a documented methodology or internal manual for the licensing procedure apart from the application form, which guides the GGC to check relevant data, including compliance with the general requirements of the Gambling Act.⁷⁴ In the view of the authorities this approach is proportionate with the low number of new licence applications received. Nevertheless, this could lead to some issues going unnoticed (e.g. in one case presented onsite to the AT, certain issues had been overlooked, such as the identification of all the beneficiaries of a trust).

417. Applicants must also declare any criminal or administrative sanctions, or investigations. The GGC checks this information through the GCID (including checks with Interpol databases) and liaises with other authorities when needed. The GGC also considers information from third-party reviews⁷⁵, media and other open sources. According to the authorities, the background verification was already being conducted applying the Gambling Act before relevant requirements were introduced under the POCA.

418. The GGC cooperates with relevant foreign counterparts (primarily with the UK) where necessary on licencing. This seems appropriate considering the number of operators and the country of origin or residence of the clients. The GGC has also provided certificates relating to operator approvals to authorities in other jurisdictions (US, Malta and Italy).

419. Regarding unauthorised activity, there is a certain overlap between certain financial products and gambling (e.g. regulated investment funds where the underlying investment methodology is bet prediction). A handful of such schemes when referred to the GGC by the GFSC have been rejected.

420. There have been many attempts to bypass the GGC when establishing gambling services providing companies in Gibraltar. The CHR checks declared activities with the GGC and rejects the relevant application. The AT was provided with case examples illustrating effectiveness in this matter. The GGC also monitors the market with the cooperation of the OFT and Department of Employment, telecom regulators and uses open source information to detect unlicensed activities.

RSC

421. Persons who wish to be admitted and enrolled as either a solicitor or a barrister in Gibraltar must apply to the Chief Justice.⁷⁶ The admission process in Gibraltar includes an interview with the Admissions and Disciplinary Committee (a three-person panel which includes the Attorney General as chair) to determine whether the applicant is fit-and-proper. There is no formal methodology to indicate the risk factors and criteria that must be considered. The Committee provides a report to the Chief Justice, who takes the final decision in a public hearing.

422. All first-time applicants are checked against criminal records, but this does not apply to legal professionals who are already licenced. Questions also arise as to whether criminals are effectively prevented from holding positions as legal professionals. In one case, a legal firm had been referred to the disciplinary committee of the RSC in 2017 for alleged involvement in ML,

⁷⁴ See Schedule 1 of the Gambling Act

⁷⁵ From gaming associations

⁷⁶ Applicants must have completed their legal education in England, Wales, Scotland, Northern Ireland or Ireland and/or been admitted to practice in those countries.

based on a reference made by a third-party (a NPO). No conclusion had been reached by the time of the on-site and no suspension of activity had been imposed by the Chief Justice.

423. Legal professions conducting activities under POCA were identified based on the RSC questionnaire sent to all legal firms and sole practitioners in Gibraltar (in 2017). Out of 39 firms, 30 identified themselves as providing clients with services covered by POCA. No subsequent similar exercise has taken place.

OFT

424. The OFT is responsible for licensing dealers in high value goods, HVDs (including DPMSs), REAs, accountants and tax advisors.⁷⁷

425. Dealers and REAs were requested by the OFT to complete and return a survey with information on the business, its BOs directors and managers. Once information was gathered, existing HVDs and REAs were checked (including criminal checks and AML/CFT sanctions through a MoU with the GFU and a procedure with the RGP) and initially risk-scored by the OFT.

426. The OFT has developed a formal procedure for authorisation. Although the procedure indicates that it applies only to *new* licence requests, the OFT declared that in practice it is applied to all existing licences. The OFT has put in place an AML/CFT Team (2 persons) that works closely with the Authorisation Team (AT) of OFT and performs due diligence, including criminal records checks on individuals. All REs are required to submit annual reports in which they present any changes to the business's management. Although the procedure specifies that it only applies in case of transfers of business, new owners or managers are in practice also subjected to the same fit-and-proper checks.

427. In relation to unlicensed activity, the OFT has cooperated with the Income Tax Office and the Department of Employment, apart from checking general information in media and public sources.

6.1.2. Supervisors' understanding and identification of ML/FT risks

428. The GFSC and GGC have a robust understanding of risk. The OFT's risk understanding is in its nascent stage, although it is developing fast. All authorities are part of a bi-monthly inter-agency meeting in which ML/FT related matters are discussed.

429. The GFSC and OFT have developed documented methodologies to assess the ML/FT risks posed by each reporting entity but the factors taken into consideration, as well as the data feeding into the formula need some improvements (see par.433). The GGC has a basic risk scoring methodology which considers the size and number of SARs, geographical outreach and a review of each operator's own risk assessment but it is not documented, and no clear formula applies. The RSC has not developed a methodology and has not categorised entities in respect of their ML/FT risk. In the case of accountants and tax advisors, the shortcoming results from the absence of dedicated supervision.

GFSC - FIs, TCSPs, DLTs, auditors and insolvency practitioners

430. Overall the GFSC has a robust understanding of the inherent risks of the REs. It has taken additional steps in the last 5 years in its overall assessment of REs to emphasise the ML/FT risks, and this forms the basis for its supervision. The GFSC also provided input into both the 2016 and

⁷⁷ Accountants perform only book-keeping activities and there was only one independent tax advisor in the process for licensing at the time of the on-site. Also, supervisory activity for accountants and tax advisors is performed by the Finance Secretary, not the OFT.

2018 NRA. This included gathering data from REs through its annual Financial Crime Return.⁷⁸ The GFSC's risk methodology considers the findings of the NRAs (e.g. recent thematic reviews have been driven by the findings of the 2016 and 2018 NRAs).

431. The general risk management framework developed by the GFSC in 2016 focuses on two risk categories: Strategic and Operational; and Regulatory, the latter including the Financial Crime risk broken down by the impact and likelihood for each type of sector (e.g. Banks, TCSPs, DLT providers). Each risk identified is enrolled in the risk register and attributed to a series of metrics (KRI – Key Risk Indicators). These are based on discussions and consultations between different departments in the GFSC which take place at regular intervals (usually monthly) or in the event of any trigger events but those discussions have not been recorded or documented.

432. So far as virtual currencies and DLT providers are concerned, the GFSC conducted 2 discovery exercises addressing all the sectors that might be involved in DLT (including some that are not under the GFSC's supervisory umbrella, such as legal professionals) with respect to any ICO activities they might perform. Although ultimately there was no documented assessment of this sector, the GFSC considers those exercises to have been useful because they led to a proper understanding of the risks involved by the sector and have enabled the GFSC to work more closely with those firms with a higher exposure to virtual currencies.

433. Up until 2017, the GFSC considered ML/FT risk when scoring supervised entities but ML/FT was not necessarily the driver for scoring or supervision. In 2017, the GFSC developed a standalone Financial Crime Risk Methodology to assess the specific ML/FT risk posed by each supervised entity. The Methodology has a 2-step approach. Initially it focuses on quantitative data provided through the FC Return to determine the inherent risk profile for each entity using 4 risk categories (*Customer, Product, Interface, Country*), together with a 5th (*Other risks*) which includes any other financial crime risk such as bribery, fraud, tax evasion or corruption. The methodology considers both absolute values and percentages when calculating different levels of risk. For example, the absolute number of PEPs in the client base: if an entity has more than 75 clients classified as PEPs, then the '*customer risk score*' is high. But if the percentage of PEPs is less than 25%, then the '*customer risk score*' is low. Also, in case of customer risk, the analysis includes the number of '*high risk customers*' and risk scored by each RE. Although the GFSC advised that it considered the criteria used by REs to profile their customers, the overall risk score could be diverted. For example, for a firm that has a high-risk appetite and therefore a low number of high-risk customers, the overall risk attributed by the GFSC will be lower. Although the absolute values method and the percentages values method can give rise to contradictory risk assessments, the GFSC advised that the final risk scores which are used to determine the level and frequency of supervision are only those based on percentage values and the scores based on absolute values are for information purposes only.

434. After an on-site visit or desk-based review in which the controls and procedures of the entity are assessed, a residual risk is calculated for each category of risk (product, customer, interface and country) and the highest level of the 4 will be considered when calculating the overall level of risk.

435. Since the introduction of the new methodology, the TCSP and E-money sectors have been reviewed and assessed as described above by way of thematic reviews. Apart from these, only a handful of other entities have been risk assessed under the new Methodology, of which 2 were banks; these were due to trigger events and both had their risk downgraded. All other firms remain risk profiled under the previous risk methodology but are scheduled to undergo new assessments in the near future. A thematic review for the *Bureaux de Change* sector is currently

⁷⁸ FC Return – an annual questionnaire that each supervised entity has to fill in and return to the FSC.

underway; a thematic review for the banking sector is scheduled to take place in 2019 and a thematic review for securities and funds will be in 2020. The authorities mentioned that this approach will be considered in assessing all sectors.

Other DNFBCPs

GGC

436. The GGC provided input for the first two iterations of the NRA, published in 2016 and 2018, and has a good understanding of the inherent ML/FT risks posed by the gambling sector and these is importantly overlap with the risks of cheating, collusion and fraud to which the sector is more exposed⁷⁹. The GGC's input was facilitated by the fact that GGC received, up until the end of 2018, SARs in tandem with the FIU.

437. The main driver in assessing risk is the size of the operator. This approach was explained by the fact that the size includes factors such as a customer, jurisdiction and product (the bigger the operator is, the larger is the base of different clients, geographical range and product offering). Other factors are then taken into consideration and given weight, such as the interface, with poker platforms for remote gambling being recognized by the GGC as posing an additional ML/FT risk. Country risk is also regarded in some respect, although it became apparent on-site that countries were considered to be high risk based not only on FATF or UK Treasury lists, but also on ad-hoc internal considerations rather than documented assessments.

438. At firm level, a basic methodology which considers both risk factors as described above together with quantitative data, received through questionnaires, is used to assess the level of risk different operators pose. The GGC also reviews each operator's own AML/CFT risk assessment.

RSC

439. The RSC was not engaged in drafting the 2016 NRA but was involved in drafting the 2018 NRA, with which it agreed without providing additions. The RSC has not conducted any separate assessment of the sector and indicated during interviews that the main ML/FT risk for legal professionals was their unwilling and unknowing enabling of criminal activity, especially when assisting real estate transactions. There are no formal procedures or risk methodology in place to assess the sector.

OFT

440. The OFT has a general understanding of the risks posed by the entities it supervises and acknowledges the threats but considers these to be low because of the entities' size and the products offered. Nevertheless, there is no documented ML/FT risk assessment of the sectors.

441. HVDs and REAs send annual reports to the OFT with statistics on the following topics: cash payments received or rejected in the previous year; number of internal reporting and SARs sent to the GFIU; information on the AML/CFT policies; self-risk assessments conducted in the previous year and the vulnerabilities considered.

442. Collected data is used by the OFT to identify any inconsistencies or suspicious activities in general to understand the different activities in these sectors, how they operate and their inherent ML/FT risks. The report form specifies that it is to be sent 9 months after the end of the financial year (the same deadline as for tax returns). The OFT has nevertheless advised the AT that in practice, the delay only applies to certain financial information so that the OFT may benefit from using audited financial data.

⁷⁹ This has also led to an over reporting activity of ML/FT STR from gambling operators.

443. The OFT also uses Risk Matrices and has assessed regulated entities based on the initial results of their HVD/REA surveys and on consultation meetings or first onsite visits. At the time of the onsite, the OFT was in the process of finishing the drafting of an “on-going risk scoring policy” different from the one used for the initial assessment of entities. This considers technical and effectiveness issues and is to be applied on a regular basis when receiving documents and reports from entities, after having contact with the entity or receiving relevant information about the entity.

6.1.3. Risk-based supervision of compliance with AML/CFT requirements

444. The supervisory authorities enhanced their supervisory activities in AML/CFT matters after the adoption of the POCA and SBPR. The GFSC applies a targeted risk-based approach (RBA) to AML/CFT issues. The OFT also follows a RBA approach, although it must be noted that the OFT received its supervisory function in AML/CFT matters only recently. The GGC’s supervisory approach in AML/CFT issues also follows a RBA approach but after (and as a result of) the adoption of the new POCA, in a more systematic manner. The GGC bases its supervisory attention on a firm’s size rather than on a more nuanced understanding of ML/FT risks and this raises some concerns. The RSC has launched a discovery exercise in 2017 to obtain data on the entities they supervise and, on the AML/CFT risks posed by each regulated business. In addition, the RSC has started to develop a risk based supervisory approach.

GFSC - FIs, TCSPs, DLTs, auditors and insolvency practitioners

445. The GFSC makes no distinction between FIs and the DNFBPs under its supervision and applies the same methodologies to all supervised entities in form of desk-based reviews and on-site inspections.

446. Each entity is attributed an AML/CFT focused supervisory plan. This is based on the residual ML/FT risk score (calculated as described under Core Issue 3.2 through the Financial Crime Risk Methodology) with a maximum 3-year supervisory cycle for AML/CFT. The higher risk entities are reviewed and assessed more often, with an on-site inspection every year and with periodic communication with the firm to manage any high risks identified. The calendar is set by the Financial Crime Unit and is not dependent on another team's supervisory calendar, although where possible it considers other supervisory activities. It is difficult to assess the effectiveness of this new approach given the fact that it has only been adopted recently. Before 2017 risk-based supervision was focused on the general risk of an entity; this took into consideration the ML/FT risks but was not driven by them.

447. The number of on-site and off-site inspections that captured AML/CFT issues does not seem sufficient given the size of Gibraltar’s financial sector. The GFSC explained that prior to 2017 more on-sites and desk-based assessments were conducted and these included a review of the firms’ AML/CFT systems and controls, but that review was not the sole purpose of the assessment and was not recorded or included in the statistics.

448. After 2017, the supervisory efforts were focused on Thematic Reviews (TCSPs and E-Money) and this explains the increase in the number of on-site and desk-based assessments. The choice of TCSPs and E-money providers for a thematic review was based on the risks identified in the 2016 NRA and reflected in the action plans that were adopted pursuant to the 2016 NRA.

Table 33: AML/CFT Inspections 2014-2018 (including inspections which formed part of thematic reviews)

	2014		2015		2016		2017		2018	
	FIs	DNFPB	FIs	DNFPB	FIs	DNFPB	FIs	DNFPB	FIs	DNFPB
No. of Reporting Entities	196	76	214	99	219	98	246	95	235	94
On-site inspections that covered ML/FT	2	17	5	0	6	3	11	26	7	6
Total inspections that covered ML/FT (on-site and off-site)	14	17	5	1	7	3	11	26	8	32
ML/FT Violations	14	17	5	1	7	0	11	24	8	26
Supervisory notices and guidance documents	10	3	10	3	10	3	25	6	24	4

BOX 16 – Thematic Reviews

As part of the new financial crime oriented supervisory approach, the GFSC had undertaken (by the time of the onsite visit) 2 AML/CFT Thematic Reviews to assess how entities had implemented AML/CFT systems of controls and how they were being applied in practice. The Thematic Reviews captured TCSPs and E-Money providers primarily because those sectors were identified as posing a higher ML/FT risk in the 2016 NRA and the action plan set to address these risks included carrying out a thematic review of the sector.

The TCSP Thematic Review consisted of 26 on-site inspections carried out in Q4/2017 and 31 subsequent desk-based reviews. The on-site inspections were usually carried out by 2 persons from the AML/CFT Team and were lasting 2 days. The results were made public in June 2018. The E-Money Thematic Review consisted of 4 on-site visits, capturing the entire market, carried out in Q4/2018. The results were published in February 2019. Overall, the TCSP thematic review exercise took 1 year to complete, while the E-Money Thematic review lasted 6 months.

From the examples provided by the authorities, the inspection team consisted of 2 to 3 people both from the Regulatory Division and the AML/CFT Unit and the onsite visits lasted 2 or 3 days for each firm. The discussion was of the following issues: corporate governance, compliance, client acceptance and risk profiling, financial crime and AML/CFT procedures (including monitoring and reporting of STRs). The inspection team also randomly selected and reviewed client files, including KYC documents, correspondence and bank statements.

A series of shortcomings were discovered during the on-site visits and reviews. Following the Thematic Reviews, 5 TCSPs were placed under intensive supervision and at the time of the onsite they were in the process of addressing the identified deficiencies. No other sanctions were imposed.

One E-Money provider was referred by the Supervision team to Enforcement and in December 2018 the case was escalated to the Enforcement and Regulatory Interventions Committee. The decision was to draft a Warning Notice with deferred effect that would become enforceable if the firm would not follow on its remediation plan and deadlines. The firm currently falls under the responsibility of the Intensive Supervision Team who continues to work with it to remediate the identified failings. Further onsite follow up visits are scheduled. Up to the visit of the AT, the firm had followed up on its remedial plans.

publications of the results included a summary of the main findings relating to CDD, on-going monitoring, risk assessments, and also the best and poor practices. The E-money Thematic Review also included dedicated assessments of corporate governance, training, outsourcing and PEPs.

449. The Financial Crime Procedures Manual (issued to assist in the new AML/CFT supervisory approach) standardises to a certain level the pre-assessment work and on-site visits, and indicates a list of things which must be reviewed (e.g. client file samples to verify adequacy of CDD, check the number of internal SARs, policies, procedures and controls in place, including how they are applied etc.).

450. The GFSC has also established an Intensive Supervision Team, with the objective of supervising firms which either pose greater regulatory concerns or appear to be facing significant challenges in the near future. After the thematic review of the TCSP sector, 5 new entities were placed under intensive supervision (one entity had already been placed under intensive supervision already previously).

451. The GFSC’s total number of staff has doubled in the last 5 years, to 96 people The GFSC advised that they have an agile HR approach and that staff move between departments to address any resource issue. The AML/CFT Team is composed of 5 staff members, but there has been a number of cases where their colleagues from other departments assisted them. The authorities have adequate numbers of individuals with relevant skills in place for each team. All staff receive in house training provided by members of the AML/CFT Unit, who in turn receive external training.

Other DNFBPs

GGC

452. The GGC’s supervisory approach, including in AML/CFT matters, has been primarily based on considerations such as the size of the operator, the number of SARs received (up to the end of 2018) and on any perceived disproportionality between these two figures (e.g. where it is apparent that, given the size and scale of a licensee, there does not appear to be a proportionate number of SARs received).

453. Inspections are performed by gambling officials who have all undergone AML/CFT training and AML/CFT forms part of the broader supervisory process. The number of dedicated on-site inspections increased substantially in 2017 and visits covered all areas of ML/FT (e.g. assessing the overall governance, controls and procedures to client file sampling, including how sanction lists have been checked by operators).

454. The number of on-site inspections dropped heavily, after the peak in 2017, while the number of desk-based reviews increased. The authorities explained that this arose from the adoption of a more structured approach and from focusing on the risks of each operator.

455. No AML/CFT violations have been recorded in the statistics, although authorities mentioned that they discovered certain shortcomings during their inspections, e.g. a case when one operator did not carry out adequate checks on the source of funds of a client. However, the GGC’s understanding was that such violation was not serious enough and that is why it was not reflected in the statistics. The authorities acknowledged not only that there was a lack of more detailed statistics but also that there was a need to improve.

Table 34: On-site Inspections

	2014		2015		2016		2017		2018	
	B2C	B2B	B2C	B2B	B2C	B2B	B2C	B2B	B2C	B2B
No. of REs	22	8	23	12	20	11	17	13	16	17
On-site inspections that covered ML/FT	22	8	23	12	20	11	35	20	7	0
Total inspections that covered ML/FT	22	8	23	12	20	11	35	20	37	16

(on-site and off-site)										
------------------------	--	--	--	--	--	--	--	--	--	--

456. There is no formal calendar for future inspections or follow-ups. The GGC considers that the relatively small size of operators allows for onsite visits to be easily arranged and for follow-ups to be readily organised, although it is acknowledged that a more structured approach would be beneficial.

RSC

457. An awareness raising introductory visit was performed by the RSC to all legal professionals who fall under the requirements of POCA and these visits included checking samples of client files. AML/CFT policies were provided to the RSC either before or after the on-site visit and were desk based reviewed. None of these actions have been transposed into a formal procedure. There has also been no documenting of the findings apart from the exchange of emails/mail. Lawyers' firms have not been risk assessed in respect of their ML/FT risks and a supervisory plan has not yet been developed. The RSC nevertheless indicated that law firms will be revisited, and the programme of such visits will be based on the size and complexity of those firms.

Table 35: On-site Inspections

	2017 ⁸⁰		2018	
	REA	HDV	REA	HDV
No. of REs	51	33	54	33
On-site inspections that covered ML/FT	1		1	3
Total inspections that covered ML/FT (on-site and off-site)	1		34	3
ML/FT Violations	1 ML/FT		30 ML/FT	0
Supervisory notices and guidance documents	0	5	11	5

458. The OFT has performed a number of inspections (see Table above) for AML/CFT purposes. HVDs were visited on-site, while REAs were primarily supervised through the desk-based review. In addition, a general meeting was held within the scope of the Project Nexus. The OFT holds discussions during inspections with both senior managers and front-line staff, setting out various scenarios in order to assess their ability to detect and manage a suspicious activity. Internal systems of control and AML/CFT policies were also analysed during onsite inspections as well as any computerised system for record keeping.

459. In relation to sanctions list, the OFT is in course of updating the Guidance Note with respect to TFS and client screening, to incorporate relevant regulatory updates and take those into consideration during their inspections.

460. After the initial risk scoring, the OFT mentioned that 2 entities were revisited, due to adverse information which triggered a rise in the level of risk and giving rise to the need for on-site inspections. Both entities were re-scored after the inspections. While this development took place after the AT's on-site visit to Gibraltar, it is nevertheless an indicator of the RBA's application of supervision.

6.1.4. Remedial actions and effective, proportionate, and dissuasive sanctions

461. Whilst the authorities in the vast majority of cases had at their disposal a broad range of sanctions which could be imposed on entities they supervise and on individuals (examples of the

⁸⁰ Prior to 2017, OFT had no powers for AML/CFT supervision, therefore no statistics exist.

different enforcement sanctions have been provided to the AT) the authorities mostly relied on remedial plans and supervisory notices and guidance. Such an approach (i.e. awareness raising before the imposition of sanctions) might seem reasonable when it concerns newly appointed supervisors (such as the OFT and RSC) but for FIs and TCSPs which have been subject to AML/CFT requirements prior to the POCA, one would expect that a lack of AML/CFT compliance would trigger more dissuasive sanctions – especially if serious shortcomings were identified.

462. There have been 2 settlement agreements presented by the GFSC in recent years which included both financial penalties and individuals stepping down. No sanctions were imposed by the GGC in either case. Therefore, in the view of the AT, the authorities could not fully demonstrate the proportionality or dissuasiveness of the sanctions applied in practice.

GFSC- FIs, TCSPs, DLTs, auditors and insolvency practitioners

463. The GFSC has a broad range of sanctions it can impose on entities it supervises. Enforcement actions can be taken against a firm, an individual or both, and may range from taking remedial action, giving written warnings and imposing fines up to the withdrawal of a licence or revoking individuals.

464. Gibraltar is currently undergoing a broader financial services legislative reform programme which is due to be completed in the near future. One of the expected reforms will include setting up a special department to oversee the enforcement of sanctions.

465. For the period analysed, remedial actions in the form of guidance and notices were applied more frequently than other sanctioning tools. In the period 2014-2018 there have been more than 100 AML/CFT violations detected,⁸¹ but only 1 financial penalty was imposed (in 2018) in the sum of GBP 250,000 (by way of an agreed regulatory settlement). This sanction was imposed on an E-money provider which had major breaches in its AML/CFT controls.

466. One other case included AML/CFT breaches and unlicensed activity and concluded with a regulatory settlement (a penalty of GBP 10,000 and 2 officers stepping down permanently) was presented to the AT. A number of public warnings and closures of businesses because of unauthorised activity have been issued by the GFSC in the last 5 years.

467. The authorities explained that they consider their actions applied to have been proportionate to the shortcomings identified through their inspections. They also consider their approach to have been compliant with the GFSC's Enforcement strategy and with FATF Guidance. The strategy stipulates that where a firm accepts and acknowledges the fact that it failed to comply with regulatory requirements, and if the breach does not pose a serious or persistent risk to regulatory objectives, a matter can be appropriately resolved by way of a supervisory response, which, apart from intensive supervision, also includes guidance and remedial action plans.

468. Supervisory responses as described above were also applied as a result of Thematic Reviews. As shown in Box 19, 5 TCSPs were placed under intensive supervision and one E-Money provider was referred to the Enforcement Department with a proposal to issue a warning. The warning was not issued, but the firm was put under intense supervision. At the time of the on-site visit, the firm was still in the process of addressing the identified deficiencies.

469. Nevertheless, the shortcomings discovered in the Thematic Reviews of 2017 and 2018, as well as other shortcomings identified during prior inspections, include some issues which are fundamental for AML/CFT compliance. These shortcomings include: not screening clients against proper sanction lists; not performing CDD on all required individuals, including the BO; onboarding clients prior to all CDD being performed; not screening for PEP status or not applying

⁸¹ See Table 28

EDD when identifying PEPs; not performing adequate or sufficient on-going monitoring; not having procedures updated or there being even a lack of any regulatory knowledge of AML/CFT requirements. It has to be noted that that these basic requirements were not introduced by POCA but have been in place long before its introduction.

470. The AT notes the discrepancy between the issues identified through thematic reviews/other inspections and the number and type of actions undertaken. The authorities mentioned that all entities which have undergone a thematic review were explicitly warned that, should the similar shortcomings be identified in the future, the GFSC's response would be more drastic. The AT finds that such an approach brings into question the effectiveness and dissuasiveness of GFSC's supervisory regime and sanctioning policies. It also touches upon the lack of impact that supervision has had on compliance with the AML/CFT requirements.

471. No individuals were formally sanctioned by the GFSC in the period under review, although some have stepped down as a part of the regulatory settlements. The GFSC advised the AT that it had, in the past, imposed changes in management and the MLRO, albeit that this was not included in the official statistics.

BOX 17 – WCHL Case

W.C.H.L. is a Gibraltar E-money provider which was licensed in 2010. The GFSC identified a number of concerns regarding the firm's effectiveness of AML/CFT controls and the firm acknowledged and accepted that in several respects its AML/ CFT systems and controls during a part of the period from 1 January 2017 to May 2018, fell below the standard expected for regulatory purposes. It voluntarily agreed not to take on any new business in February 2018. It also paid £250,000 by way of an agreed regulatory settlement in December 2018. The Chief Executive Officer, Non-Executive Chairman and Compliance Officer/MLRO of the firm also voluntarily stepped down and agreed with the GFSC not to seek any notifiable position for the 2 years, unless and until they undertook a programme of continued professional development in relation to AML/CFT. Officially, the GFSC did not make any adverse finding of their fitness and propriety.

472. Prior to any decision notice, a settlement discussion can take place at any time in order to reach a regulatory outcome with the firm or individual involved.

Other DNFBPs

GGC

473. Prior to the adoption of POCA and the introduction of the SBPR⁸², license sanctions or cancellation were the only material sanctions available to the GGC. This deficiency has now been addressed (see TCA C.27).

474. Since the introduction of the SBPR, the GGC has had remedial actions applied in 3 cases. These included the divestment of profit by licensees and the sending of a warning letter. These cases were nevertheless not directly linked to breaches of the AML/CFT requirements. The GGC considers that the findings of its on-site supervisory inspections required only remedial action in the form of advice – some of which was given on the spot. They considered that this was sufficient to achieve the desired outcome. In their opinion, the breaches identified did not warrant sanctioning. No violations of AML/CFT issues have been recorded in the GGC's statistics.

RSC

475. The RSC has undergone one round of on-site supervision in 2018 which covered all 30 firms and sole practitioners who offer services under the POCA. 3 law firms in total were found to have AML/CFT deficiencies (mainly in their internal policies) and these were provided with feedback

⁸² Supervisory Bodies (Powers) Regulations 2017

via email. Two of those firms complied swiftly, and the other was given more time as the person in charge of AML/CFT had health issues and was abroad for a longer period. No sanctions (that might have included striking off the registrar or suspending the activity) were applied in practice.

476. In 2017 one law firm was referred to the disciplinary committee of the RSC for involvement in ML, based on a reference made by a third party (a NPO). The case is still pending, and no suspension of their activities has yet taken place.

OFT

477. The OFT has not imposed any sanction by the time of the on-site visit. This is understandable given the fact that the entities under their purview are still in the early stages of adapting to new requirements under POCA. (REAs and HDVs were not covered for AML/CFT purposes previously).

478. The OFT considers that there will be a shift from the present non-sanctioning approach in the future as the market becomes more mature in terms of AML/CFT compliance. In support of this submission they advanced that during the on-site visit one HVD had been undergoing a sanction enforcement process for breaches identified in respect of a CDD application and the risk assessment of a transaction. The penalty administered was a warning notice. The OFT considered publication but decided that this would be disproportionate given that the entities were still on-going adjustment to the new requirements brought in by POCA and its guidelines.

6.1.5. Impact of supervisory actions on compliance

479. The supervisory authorities are well respected, and the majority of entities interviewed on-site were aware of their obligations to comply with the AML/CFT requirements, including with the recent changes in the regulatory framework. This finding confirms that the supervisors' awareness-raising efforts have had a positive impact. On the other hand, one has to bear in mind that supervisory and regulatory actions with regard to AML/CFT were enhanced only in recent years. This fact, in conjunction with the finding that enforcement has been applied only in a few instances, mostly in the form of the remedial plans, suggest that the effectiveness of supervisory actions on compliance was achieved only to some extent.

GFSC - FIs, TCSPs, DLTs, auditors and insolvency practitioners

480. The GFSC has established good communication with the entities it supervises. It regularly follows up on these entities' compliance with the supervisory and remedial actions imposed on them. The GFSC also presented cases where remedial actions included the appointing of new directors⁸³ with specific AML/CFT experience, staff training and awareness, and close follow up by the GFSC, sometimes even on a daily basis, to verify the implementation of the remedial plans.

481. Where the findings for a particular on-site visit are relevant to other entities, the GFSC brings them to wider attention. This has been observed especially in the case of thematic reviews undertaken recently, where results – including best and poor practices, have been made public. This measure is expected to have a further positive impact on compliance, as other types of FIs supervised by the GFSC can compare the results of the findings, including best and poor practices, against their own activities ('self-inspection') thereby keeping themselves better informed of what the regulator expects from them and on what it is particularly focused upon.

482. After the thematic review of the TCSP sector, 5 out of the 58 firms inspected were placed under an intense supervisory plan to monitor their compliance. One TCSP was placed under intensive supervision prior to the visit. At the time of the on-site visit, these firms were at a

⁸³ Although there were no individuals formally revoked

different stage of compliance and of implementation in their remedial plans. The GFSC also presented to the AT other cases in which regulated entities which had been in breach of their AML/CFT requirements were implementing their remedial plans and, as a result, achieved compliance.

483. Nevertheless, given the type of breaches discovered in the last few years, as detailed in Core Issue 3.4, it is questionable whether the GFSC's actions, especially those which took place before they increased focus on AML/CFT and developed dedicated supervisory tools (e.g. FC Risk Methodology, the use of Thematic Reviews) were effective enough as to ensure compliance of regulated entities.

Other DNFPs

GGC

484. The GGC is also intensively involved in the follow-up process of ensuring the implementation of remedial actions and has established very good lines of communication with the sector it supervises. In 2016, the GGC carried out a desk-based review of operators' AML/CFT policies and provided individual feedback to each of them. The GGC advised the AT that it had observed concrete actions of operators, in response to recent inspections. There had been increased resourcing and re-structuring of governance arrangements, for example an increase of staff in the due diligence teams of the gambling operators and improvements in their own risk assessments which became more comprehensive.

RSC

485. It seems that, given the small size of the jurisdiction and the low level of violations identified in inspections, legal professionals tend to apply swiftly the recommendations provided by the RSC. In all 3 cases in which AML/CFT breaches were discovered, follow-up actions were taken by the RSC. Nevertheless, as only one round of supervisory engagements has taken place, the impact of supervisory actions is yet to be observed.

OFT

486. The OFT is closely involved in assuring compliance in the sector, also through follow up actions with regard to the level of compliance of the entities under its supervision. The OFT's initiatives concern letters to the regulated entities under their purview which point out that sanctions might follow in case of non-compliance and include other information and documents to better steer the obliged entity through the entire process. In addition, the supervision is executed via systematic onsite visits, the production of annual reports and via regularly updated Risk Score AML/CFT Matrices for each entity as per their Business Risk Assessment policy.

6.1.6. Promoting a clear understanding of AML/CFT obligations and ML/FT risks

487. Overall, the supervisory authorities have appropriate levels of engagement with their REs when it concerns compliance with the AML/CFT requirements. This engagement has intensified in last two years. In the financial, TCSPs and gambling sectors, where supervisors have a long history of engagement and where products are more complex, communication tends to be more intensive, albeit with a one-to-one approach rather than through associations. For other DNFBPs, communication has mainly taken the form of an introduction and guidance, but this is understandable given the fact that those entities have only recently been covered by AML/CFT supervision.

GFSC- FIs, TCSPs, DLTs, auditors and insolvency practitioners

488. Following the transposition and implementation of the First Money Laundering Directive in 1990, the GFSC developed the AML/CFT Guidance Notes (AMLGN) in 1996. The AMLGN were reissued in 2016, following the adoption of POCA, which transposes the 4th AML Directive. The Guidelines have been updated several times, with the latest update in February 2019. The information on all changes made therein was sent to all regulated entities.

489. Another important engagement with the industry began in 2017, when the GFSC started to gather annual data from all market participants through the FC Return Questionnaire. As the authorities informed the AT, this exercise brought attention to certain misunderstandings by the REs on some data required, particularly in the case of *bureaux de change*, and TCSPs. These considerations were addressed through direct communication with the sectors and additional information was then provided to them, resulting in improvements in the data submitted by these sectors. Moreover, all REs were notified that the questionnaire would be submitted to them on an annual basis. It would require comprehensive and accurate data, meaning that a data extraction exercise would need to be performed by the REs at the end of each year.

490. As confirmed by the majority of REs met on-site, the GFSC is responsive to the enquiries it receives. The GFSC's AML/CFT Supervision team also has a dedicated email address to facilitate communication from regulated entities.

491. Another good example of the GFSC's engagement with the sectors it regulates was the publication of the results of the Thematic Reviews undertaken, including best and poor practices which may serve as guidance for all types of entities. Those documents were published on the GFSC's website. Only the sectors covered by the thematic review were notified about this publication, although the issues raised had a broader range of potentially interested recipients.

492. The GFSC carried out various industry engagements to raise awareness on AML/CFT matters, including training seminars, workshops, 'Dear CEO' Letters, emails and newsletters to REAs.

493. When the FATF issues public statements and country risk updates on high risk jurisdictions, the GFSC publishes this information on its website and advises all its licensees via email.

494. Overall, in the last two years the effectiveness of the GFSC's communication has increased. The GFSC is to be commended for the efforts undertaken to carry out the awareness raising activities (see also the Core issues 3.4 and 3.5).

DNFBPs

GGC, OFT and RSC

495. The GGC, the OFT and the RSC maintain a good relationship with their regulated entities. Given the size of the jurisdiction, communication is good, and feedback is often offered in a direct communication, which allows additional queries at short notice. All three supervisors developed, inter alia, sectoral Guidelines including different AML/CFT forms and presentations, with the aim of better informing the REs on relevant AML/CFT requirements.

Overall conclusions on IO.3

496. **Gibraltar is rated as having a moderate level of effectiveness for IO.3.**

7. LEGAL PERSONS AND ARRANGEMENTS

Key Findings

- a) The risk of legal persons and arrangements misuse for ML/FT purposes is understood only to some extent by Gibraltar. Although the NRA considers the risk inherent to TCSPs in their creation and management of legal persons and arrangements and the some types of activities by legal entities (LEs), no exercise has been conducted to specifically consider how the legal persons and legal arrangements, particularly those that serve as asset holding or asset protection vehicles, have been used to disguise ownership or to launder the proceeds of crime, or if there are inherent vulnerabilities to those LEs and arrangements.
- b) Gibraltar has taken a number of measures to prevent the misuse of legal persons and arrangements for ML/FT purposes, including establishing the Register of Ultimate Beneficial Owners (RUBO), prohibiting bearer share warrants and subjecting TCSPs, which are used for setting up legal persons and arrangements, to a licensing and comprehensive regulatory regime. However, important issues remain, which pose an inherent vulnerability to ML and FT.
- c) Gibraltar has a robust system that allows relevant competent authorities to obtain through the CHG on timely manner and generally accurate and current basic information on all types of legal persons created in Gibraltar. Legal person's basic information in the CHG is also available to the public, for a fee. However, legal ownership information that is registered refers primarily to TCSPs acting as nominee shareholders or directors.
- d) Authorities can obtain BO information directly from REs (including TCSPs) or rely on the RUBO. The cases that were provided to the AT showed that authorities' access to BO information from REs was timely. However, there are a number of factors that can affect the accuracy and adequacy of the BO information held by REs or in the RUBO.
- e) The absence of a requirement to keep in Gibraltar minutes of the meetings of directors, the issues concerning REs' understanding of the BO and those noted in regard to BO-related record keeping (see Chapter V/ IO.4) and issues noted by the GFSC in its thematic review of the TCSPs concerning the implementation of CDD measures, create blind spots in the completeness, accuracy and reliability of information concerning BO that can affect authorities access to adequate, accurate and current BO information held by REs
- f) The limited scope of information required to be filed in the RUBO concerning trusts (the almost totality of trusts created in or managed in Gibraltar has not provided UBO information), the fact that companies can be deemed as BO, that the information provided is not verified for accuracy and that a significant number of entities have not complied with the UBO filing requirements, affects the reliability and accuracy of BO information of the RUBO.
- g) Companies House (CHG) is aware of the targeted financial sanctions (TFS) and relevant United Nations Security Council Resolutions (UNSCRs) related to terrorism and FT, and conducts checks to spot potential matches with relevant sanctions lists, in addition to checks based on the geographic risk factors. However, given the availability and widespread use for Gibraltar companies of nominee shareholders arrangements and directorship services, the lack of a requirement for nominee shareholders and directors to disclose the identity of the nominator to the company or to the register maintained by the CHG, affects also the possibility to spot potential matches with the sanctions lists.
- h) The Companies Act (CompA) provides sanctions for non-compliance with the information

filing requirements, but only in the case of late submissions and they are not proportionate or dissuasive. There are sanctions available for non-compliance with the RUBO information requirements, but not specifically with regard to the deadlines established to provide the information to the RUBO.

i) The CHG has the option to strike off a company which has not filed any annual return reports in the previous 3 calendar years, or any company or limited liability partnership that is believed to be non-operational. The very high number of such cases raises concerns related to the potential misuse of non-operational companies.

Recommended Actions

Authorities should:

a) Assess the specific ML and FT risks related to legal persons and arrangements, including how the legal persons and legal arrangements, particularly those that serve as asset holding or asset protection vehicles, may have been used to disguise ownership or to launder the proceeds of crime, and assess the specific inherent vulnerabilities to all types of legal persons that can be created in Gibraltar.

b) Given authorities' reliance on CDD performed by REs to obtain BO information, address technical deficiencies in relation to BO-related record keeping information; and ensure that TCSPs are implementing effectively CDD requirements, particularly those related to the BO. The GFSC Guidance Notes (AMLGN) should be amended to eliminate the reference to the 25% in the case of beneficiaries of trusts. Establish requirements for nominee shareholders and directors to disclose the identity of the nominator to the company or to the register maintained by the GHG.

c) As regards the RUBO, ensure that i) RFBs and trustees provide the required information to the RUBO, particularly concerning trusts; ii) envisage mechanisms (e.g. based on risk or randomly) to verify the accuracy of the information provided; iii) require trustees of trusts governed under their law to disclose UBO information to the RUBO; and iv) introduce sanctions for late filing of the information required to be submitted to the RUBO.

d) As regards the CHG, i) introduce sanctions for not providing the information to the CHG; and, ii) increase sanctions for late filings to the CHG, so that they are dissuasive (see Technical Compliance Annex).

e) Enhance mitigating measures by requiring, for example, i) all Companies to file, at registration with GHG, information on the activity they perform; ii) PTCs to register their activity with the GHG mandatorily and not only on a voluntarily basis; iii) TCSPs to keep in Gibraltar copies of the minutes directors' meeting for all LEs and arrangements created in Gibraltar and/or managed by a Gibraltar licensed TCSP; iv) limit the use of flee clauses, for example by indicating specifically the circumstances that trigger them; and v) consider requiring companies to have at least one director natural person and resident in Gibraltar.

497. The relevant Immediate Outcome considered and assessed in this chapter is IO.5. The Recommendations relevant for the assessment of effectiveness under this section are R.24-25⁸⁴.

⁸⁴ The availability of accurate and up-to-date basic and beneficial ownership information is also assessed by the OECD Global Forum on Transparency and Exchange of Information for Tax Purposes. In some cases, the findings may differ due to differences in the FATF and Global Forum's respective methodologies, objectives and scope of the standards.

7.1. Immediate Outcome 5 (Legal Persons and Arrangements)

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

498. The information on the creation and types of legal persons and arrangements in Gibraltar is publicly available on the Gibraltar's Government website (www.gibraltarlaws.gov.gi) and the CHG website (www.companieshouse.gi) including laws and guidance notes, information on registration of the private and public companies in Gibraltar and other relevant guidance on various matters. In addition, the CHG website includes information on European Economic Interest Groupings, Limited Partnerships, Limited Liability Partnerships, Registered Trusts and Private Foundations.

499. Gibraltar recognises trusts, and has several different types of trusts that are regulated or governed, in addition to common law, under various laws: the Asset Protection Trusts (APT – Bankruptcy Law); the Private Trust Company (PTC – Private Trust Company Act); purpose trusts (PT – Purpose Trust Act), which can be established for non-charitable purposes (e.g. asset holding vehicles). The Trusts (Private International Law) Act of 2015, is a firewall legislation to protect trusts established in Gibraltar from foreign laws or judgments (but not law enforcement actions). The information on these types of legal arrangements (including how to set them up) is available in relevant laws, published at the Gibraltar's Government website (www.gibraltarlaws.gov.gi).

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

500. Gibraltar has only a basic understanding of the vulnerabilities and the extent to which legal persons and arrangements created in the country can be, or are being misused for ML/FT. Although the risk related to the misuse of corporate vehicles has been assessed in the various NRAs, the comprehensiveness of the assessment is not satisfactory and there are significant differences in the conclusions reached on the overall risk posed by the misuse of corporate vehicles that can be created in Gibraltar, which cannot be easily reconciled.

501. The 2012 threat matrix (see Chapter 1 on Country's risk assessment) considered corporate vehicles and their misuse only in very generic terms, by referring to the risk of providing an additional level of opacity that could be associated to legal persons and arrangements, and placing this category, among the higher risks identified.

502. The 2016 NRA also considered the risk of misuse of corporate vehicles, noting that the speed and versatility with which Gibraltar companies can be incorporated and used could be one of the main attractiveness of their use by criminals. The 2016 NRA noted also that TCSPs may be unwitting participants in ML or FT if they fail to understand the reasons why a legal person or arrangement is being formed, and if they fail to conduct adequate due diligence on the establishment of the legal person or arrangement or to appropriately monitor the transactions for which the service is provided. However, the risk was considered "medium", without a specific analysis of the inherent vulnerabilities of the specific LE type or of the TCSPs (through which LEs are created and managed in Gibraltar), except for noting that TCSPs are licensed and regulated.

503. The 2018 NRA considered the risk inherent to TCSPs in their creation and management of legal persons and arrangements and the types of activities by LEs. The risk rating was increased and featured again among the higher risks identified by the NRA. While this assessment looked at general vulnerabilities (such as nominee shareholdings and creation of complex and opaque structures) and at the general types of activities (noting that Gibraltar LEs are commonly used both as asset holding, investment and transactions based vehicles for both the domestic as well international community), the assessment is not very specific, as it does not analyse the inherent vulnerabilities of the specific types of legal persons that can be created in Gibraltar, or

international threats and vulnerabilities associated with legal persons incorporated in another jurisdiction yet administered in Gibraltar. No exercise has been conducted to specifically consider how the legal persons and legal arrangements that can be established under Gibraltar's legislation, particularly those that serve as asset holding or asset protection vehicles, have been used to disguise ownership or to launder the proceeds of crime.

504. While supervisory authorities exhibited more awareness of the risk of LEs being misused for ML or FT, law enforcement authorities and, in particular, the GFIU's understanding of the inherent vulnerabilities of LEs and their possible misuse in concealing proceeds of financial crimes, was not satisfactory.

7.1.3. Mitigating measures to prevent the misuse of legal persons and arrangements

505. Gibraltar has taken several important measures to prevent the misuse of legal persons and arrangements for ML/FT purposes. TCSPs, which are widely used to establish and manage legal persons and arrangements (e.g. corporates, foundations, trusts and similar legal arrangements) in Gibraltar, are licensed (including for the provision of nominee shareholding and directorship services), and subject to a comprehensive regulatory and supervisory regime and subject to AML/CFT requirements.

506. In addition to having a modern system for the registration of basic and legal ownership with the CHG, Gibraltar has also established a RUBO, with information on BOs of corporates, foundations, trusts and similar legal arrangements. Corporates and LEs incorporated in Gibraltar, including foundations, are required to obtain and hold adequate, accurate and current information on the BO of the corporate or legal entity. Also trustees of an express trust are required to obtain and hold adequate, accurate, and up-to-date, information on the BO of the express trust (which, as per the definition of BO of the RUBOR, includes the settlor, the trustee, the protector and beneficiaries or class of beneficiaries, including the details of the beneficial interests and any natural person exercising effective control over the express trust). The CHG has stricken off the registry many companies that were dormant or otherwise not filing returns.

507. Bearer shares cannot be issued, and bearer share warrants have been prohibited and phased out. The list of directors and members of companies must be kept at the registered office of the company, which, according to the law, must be in Gibraltar. The registered office address must be notified to CHG as part of the application to register the company, and the provisions of a registered office is also a licensed activity.

508. However, there are several factors, described below, that make the use of Gibraltar's legal persons and arrangements more exposed to the risk of misuse for ML (and, potentially, TF) which are not sufficiently mitigated by the measures taken by the jurisdiction. Gibraltar is an IFC with a sophisticated TCSP sector. Although, according to the authorities, the number of corporations registered with the CHG has been declining over the past 10 years, there were 13709 active companies registered at the time of the onsite visit (approximately 1 every 2,5 of Gibraltar's inhabitants), out of which only 1,6% is not created and/or managed by a TCSP (these companies are mostly local businesses).

509. Most of the legal persons and arrangements that are created in Gibraltar are established to serve almost exclusively as asset holding vehicles and for protecting the confidentiality of their BOs. Gibraltar has passed several laws to diversify the offer of the legal persons and arrangements that can be established in Gibraltar and, in the case of trusts, passed firewall legislation to protect the assets held in trusts governed by Gibraltar's law. Despite the availability of different types of legal persons and arrangements, Gibraltar has introduced two additional types of LEs, the private

foundation and the private trust company, the purpose of which seem primarily related to diversifying the types of entities that can be offered as asset protection vehicles.

510. Legal persons and trusts are often created with a level of complexity, including with multi-jurisdiction layers or links to other IFCs. The assets held by these LEs and arrangements are not always kept in Gibraltar, but often in other financial centres, or there may be other links to these centres (e.g. the company may have Gibraltar-licensed TCSPs that act as nominee shareholders or directors but for a company that they have established in country A, with a bank account or investment funds placed in country B managed by an asset manager in country C acting with a power of attorney). There are situations in which Gibraltar-licensed TCSPs provide to their clients only nominee shareholders or directorship services, or act as trustees, but the company or the trust are not registered in or subject to the law of Gibraltar (particularly in the case of trusts). While these various arrangements may be put in place for legitimate reasons, such as minimizing tax burdens or protecting assets, they represent inherent vulnerabilities that increase the risk of misuse of legal persons and arrangements in Gibraltar.

511. There are other issues that affect the effectiveness of this IO. Since most of the companies are introduced by a local TCSP who takes care of the CHG registration process, the CGH relies primarily on the TCSPs for the accuracy of information. Although the CGH was fully aware of TF sanction lists and does also checks taking into account the geographic risk factors, these checks against shareholders or directors can only be done manually, as the CGH is in the course of informatising this process. Considering that, because most of the companies are introduced by a local TCSP, who takes care of the CHG registration process, the CGH relies primarily on the TCSPs for the accuracy of information, the unsatisfactory awareness of TFS sanctions regimes demonstrated by REs, including TCSPs, noted in the analysis of IO.4, increases the risk. Corporates are not required to file, at registration, information on the activity they perform (in practice, this happens only when the first annual return for the company is filed, after 16 months from registration), which leaves a blind spot on an important type of information that can be used by the CGH to classify companies based on risk.

512. Gibraltar has recently introduced private foundations and private trust companies, which are currently only very few. To mitigate the risk of misuse, it has required that one of the members of the council of the foundations be licensed, and, in the case of a private trust companies, that the company has a registered administrator. However, registered companies that act as private trust companies are not obliged to register with the CGH in this capacity. Companies are not required to maintain the minutes of the board of directors in Gibraltar, which might leave blind spots in a criminal investigation concerning such companies. A company can be engaged to act as director or shareholder of a Gibraltar company and there is no requirement for the directors or shareholders to be Gibraltar resident. Also, in the case of a foundation the council of the foundation may be entirely represented by or may be a corporate.

513. Despite the RUBO Regulations (RUBOR) established that UBO information should have been provided by September 30, 2017, authorities reported that at the date of the onsite mission, about 20% of the corporates subject to the UBO disclosure requirements, have not yet complied with it. While it was possible to determine the number of corporates that have or have not complied with the UBO disclosure requirement, given that that number can be compared with the total number of corporates entered in the CHG; the same is not possible for trusts and other legal arrangements, given that the registration of trusts with the CHG is only optional. No sanctions had been issued to those that have not complied with the UBO disclosure requirements, and no sanction is available for not providing the information within the established deadline, which affects effective compliance with the disclosure requirements. No verification is undertaken of the information provided to the RUBO.

514. Although the RUBOR clearly defines the BO as being a natural person, the forms for entering the information in the RUBO envisage also that a “*relevant legal entity*” can also be deemed as an ultimate BO for the purpose of the BO disclosure requirements (which is not in line with the FATF definition of BO, which always refers to a natural person). Finally, the possibility to consider as BO a person who holds 25% of the shares plus one, has resulted in arrangements by which an individual appears the direct owner of the shares just below the threshold, whereby the rest (75%) appears in the name of a TCSP (as nominee shareholder). Although the RUBOR specifically states that a share held by a person as nominee for another is to be treated for the purposes of the RUBOR as held by the other, and not by the nominee⁸⁵, a random search in the RUBO has evidenced cases in which the name of the nominee was entered in the RUBO as BO.

515. In the case of legal arrangements, there are additional issues. The ultimate BO disclosure requirements are limited by the fact that they do not apply to express trusts “*governed under their law*”, as per the FATF definition, but only to a trust (or similar legal arrangement) that “*generates tax consequences in Gibraltar*”. Given that the assets held by many trusts created in Gibraltar may be held abroad, this further limits the amount of BO information on trust that can be available in the RUBO. This is confirmed by the statistics provided by the authorities: as at 31 Dec 2018, there are 2,535 trusts that are managed in Gibraltar by TCSPs (these may or may not be “Gibraltar” Trusts, as the choice of the country’s applicable regime varies): however, the number of trusts which generate a tax consequence and therefore trigger the requirement to registered under the RUBOR is only 59 out of 2,535. Of the total figure only 39 are voluntarily registered on the CHG Register. There are only 23 APTs. There are also other exemptions by which trustee are not obliged to notify data on BOs, under restriction notices. Although, in the case of trust, the requirement is to notify all the relevant subjects to the trusts (that is, the settlor, the trustee, the protector and the beneficiary) a random check of the entries in the RUBO concerning trusts, showed that the only information available was of the trustee, but not the settlor or beneficiaries.

516. Gibraltar has not still implemented the 2007 MER recommendation to proscribe the inclusion of “*flee clauses*” in the trust instrument. Therefore, trusts in Gibraltar may include such clauses and Gibraltar has not introduced measures to mitigate the risk associated to these clauses. The occurrence of an event triggering the “flee” would be typically set in the trust deed, but it can be in a way that leaves broad discretion to the trustee to determine such occurrence and entitle him/her to move the assets of the trust elsewhere. These types of clauses may be abused (for example, in the case of a criminal investigation that may affect the assets vested in the trust, the trustee could move those assets elsewhere, making it more challenging to attack or recover those assets for criminal justice purposes), as it was confirmed by some representatives of the private sector. It is the Gibraltar position that a flee clause which could have the effect of obstructing a ML or FT investigation and facilitating ML or FT would be deemed to be contrary to public policy and therefore void. In any event, a flee clause designed to transfer trusteeship would not automatically transfer the trust assets themselves. The transfer of the trust assets would involve a separate non-automatic process which would need to be carried out by the trustee; and where transfer of assets would pose an ML/FT risk, existing legislation prohibits the trustee from facilitating those transfers. However, Gibraltar has not provided evidence or reference to concrete cases that can support this interpretation.

7.1.4. Timely access to adequate, accurate and current basic and beneficial ownership information on legal persons

517. Access to basic and BO information can be obtained in several ways. Competent authorities have access to CHG’s online register, through which it can obtain company and legal ownership

⁸⁵ Paragraph 10 of Schedule of the RUBOR.

information of all companies registered in Gibraltar. The RUBOR permits competent authorities, the financial intelligence unit, REs and other persons or organisations that demonstrate a legitimate interest to request information relating to an express trust, a corporate or a legal entity incorporated in Gibraltar. Authorities can rely also on their powers to obtain CDD-related information, which includes basic and BO information, directly from TCSPs (or FIs that maintain business relationships with LEs and arrangements in Gibraltar).

518. Authorities have provided the AT with a number of cases that demonstrate that they have accessed BO information related to companies through various means (e.g. request from the GFIU directly to a TCSP, via the dedicated portal, as well as cases where, pursuant to MLA requests, LEAs have obtained information. The GFSC can obtain (and has obtained) information on BO for the purpose of sharing it with other authorities. In these cases, the information provided appear to be adequate and comprehensive and obtained and provided in a timely manner, taking into account the channel used. The box below shows cases in which the information was obtained by the FIU from a TCSP (on the same day) at the request of a foreign counterpart.

BOX 18

CASE STUDY 1 - GFIU on UBO

On the 03/05/2016, a European FIU sent a request to GFIU in connection to an analysis of the information released in the Panama Papers. One of the subjects was a high-profile PEP in which the European FIU identified transactions related to a company incorporated in Gibraltar that held an account in a Gibraltar bank. The request, which was received via Egmont Secure Web, amongst other information, required company information including the details of the UBOs of the company. The request was approved and the GFIU consequently sent a request for information using a Data Protection Act form to the TCSP that managed the company on the 03/05/2016. The TCSP provided the information on the 09/05/2016. Once the information was received and analysed the data was added in a GFIU intelligence report and sent to the FIU on the 10/05/2016.

CASE STUDY 2 - GFIU on UBO

On the 04/05/2016, a foreign Law Enforcement Agency (LEA) made a request to GFIU relating to a high-profile investigation in connection to a sensitive tax evasion/ ML investigation. Media reports suggested that the subject had been named in relation to the alleged control of a company based in an offshore jurisdiction. The source of the subject's wealth was of particular interest to the investigators who believed that the subject was connected to a Gibraltar registered company Ltd. The foreign LEA requested the information on directors, shareholders, BOs of the company. On the 05/05/2016, the GFIU sent a request for information using a Data Protection Act form to the TCSP that managed the company. The TCSP provided the information required within hours. Once the information was received and analysed, the data was added in a GFIU intelligence report and sent to the foreign LEA on the 18/05/2016.

519. The box below shows cases in which the information on BO was obtained (and provided to) pursuant to an MLA request. Prior to the amendments made by the MLA Act 2018, any information that required coercive measures was carried out a Court for the evidence to be taken therein. Where a court was nominated, the Office of Advisory Counsel (OAC) would write to the Magistrates' Court to ask for a Summons to be issued for the witness to attend and give evidence and/or produce any relevant evidence. In practice the witness would prepare a witness statement and exhibit any relevant documentation, which included records that they held on the BO and then when in court, the witness would adopt that statement under oath. Following the amendment to the MLA Act in 2018, given that the bulk of the information and evidence requested is for evidence which is 'special procedure material,' production orders have since been used to obtain information. At the same time, authorities obtain a witness statement from the witness and the

witness statement exhibits all of the documents that have been produced pursuant to the production order.

BOX 19

Case Study 1 – 2016 (MLA)

A request from Switzerland was received on the 14 April 2016 in connection with an investigation into benefit and tax fraud. The accused ran a law firm in Geneva, and it was suspected that he had reduced his tax payable by not declaring all of his receipts to the authorities. The taxes evaded were said to be over CHF 4000,000. It was said that a large number of the receipts were credited to accounts that were not in the accused's accounts. There was evidence from an invoice issued by the accused that he had been paid into an account held in the name of a company registered in Gibraltar and which held a bank account in a Gibraltar bank. It was suspected that the accused was the UBO of the Gibraltar company and confirmation of the same was requested as well as business and banking information. The Royal Gibraltar Police (RGP) liaised with the witnesses, namely the bank and the TSCP who had provided secretarial services. On the 21 July 2016, when the witnesses were ready for the evidence to be taken, the OAC requested the Magistrate's Court to issue witness summons. Summonses were issued on the 27 July 2016 and the evidence was taken on the 22 August 2016 and 12 September 2016. The evidence was sent to the requesting authority by courier on the 13 September 2016. The request was fully executed.

Case Study 2 – 2017 (MLA)

A European Investigation Order (EIO) from the Netherlands was received on the 1 September 2017 in connection with an investigation into ML. The suspect was suspected of being involved in the transportation of drugs from the Netherlands to the UK and he was suspected of ML the proceeds through a Dutch company and real estate in the Netherlands and Spain. During a search in the Netherlands documents were found in connection with two Gibraltar registered companies (one was a TSCP) as well as a Spanish company. Details of the Gibraltar companies were sought in order to determine the actual ownership of an apartment in Spain and to establish if any other property had been purchased with the proceeds of crime. The UBO of the Gibraltar registered company was also sought. The TSCP had provided secretarial services to the Gibraltar registered company. The RGP liaised with the TSCP as a witness and on the 19 February 2018, when the witness was ready for the evidence to be taken, the OAC requested the Magistrate's Court to issue witness summons. A Summons was issued on the 23 February 2018 and the evidence was taken on the 7 March 2018. The evidence was sent to the requesting authority on the same day it was obtained. The EIO was fully executed.

520. While these cases demonstrate that authorities are able to obtain BO-related information also directly from REs by using their powers, there are a number of aspects that may make it more challenging for authorities to obtain adequate, accurate and current BO information in a timely manner particularly law enforcement authorities and the GFIU. An overarching challenge stems from the way companies are created and managed: this often involves complex, multi-layered ownership structures, incorporated in high-risk jurisdictions and only managed from Gibraltar through the provision of a variety of trust and company services, including off-the shelves companies, and nominee shareholders arrangements. Although these companies are created and managed by licensed TCSPs which are subject to CDD requirements, a thematic review of the sector completed by the GFSC in June 2018 evidenced as an area of concern for various firms "the use of unknown third party entities or individuals providing nominee shareholdings, where there is lack of documented rationale, oversight and monitoring of the relationship", or cases of "Due diligence not conducted on the UBO or other individuals involved".

521. Other issues include the absence of a requirement to keep in Gibraltar minutes of the meetings of directors and the issues noted in regard to BO-related record keeping and the

tendency by REs to over rely on percentages of ownership in order to establish the BO (see analysis of R.11 and IO.4), which could also create gaps in the completeness, accuracy and reliability of information concerning BO that can affect authorities access to adequate, accurate and current BO information maintained by REs and accessible by authorities. As specifically regards the BO information held in the RUBO or basic information held by the CHG, an issue is the lack of sanctions for providing the RUBO, within the established deadline, the information on BO, and the lack of sanctions for not providing the information to the CHG and, for late filings, their lack of dissuasiveness. The fact that the information contained in the RUBO is not verified for accuracy, and that not all companies have complied with the disclosure requirements, poses an additional hindrance to obtaining adequate, accurate and current BO information. It is interesting to note that one of the reasons for creating the RUBO was because LEAs had outlined “the need for information to be held such that they can clearly identify the individual(s) recorded as the beneficial owner. This requires more than just a name and an address”⁸⁶, which appears to confirm the existence of issues in obtaining in a timely manner accurate and meaningful information on BO directly from REs.

522. The authorities have the necessary powers to access this information, and LEAs stated that, in the context of a criminal investigation, it would not be challenging to obtain a court order. However, the fact that the most entities indicated that they would provide it to the GFIU only upon a production order (when one is not required for such requests from the GFIU) is of concern, as this poor awareness of the legal framework may affect the timeliness of the access, in the case in which the RE is the sole source of BO information and if a criminal investigation has not yet started.

7.1.5. Timely access to adequate, accurate and current basic and beneficial ownership information on legal arrangements

523. Authorities can access BO information related to trusts by requesting it to TCSPs (as well as FIs that maintain business relationship with trusts), relying on the CDD measures performed by such entities. In addition to the aspects noted above (see 7.1.4) that are relevant to legal arrangements, including the issues noted by the GFSC in its thematic review of the TCSPs, additional issues that may affect the timely access to adequate, accurate and current BO information concerning trusts is the limited applicability of the RUBO only to trusts that generate tax consequences in Gibraltar, and the fact that the information entered in the RUBO may only be of the trustee, but not the beneficiaries or settlor’s, which could be an indication of issues of effective implementation by REs maintaining business relationships with trusts in identifying and verifying the identities of all parties involved in the trust, and not just the trustee. The GFSC Guidance Notes (AMLGN) limits the definition of beneficiary of a trust (as BO) only to those holding 25% or more of the assets within the trust, which is not in line with the FATF standard and POCA, and can affect the completeness of the information concerning BO in the case of trust, as firms look at the operational guidance issued by the GFSC for the implementation of their AML/CFT requirements (see analysis of IO.4).

7.1.6. Effectiveness, proportionality and dissuasiveness of sanctions

524. The CompA provides for sanctions for non-compliance with the information filing requirements, but only in the case of late submissions. In this case fees can be levied, which are not dissuasive nor proportionate because, even if the authorities explained that they are tiered, they are only between GBP 17,50 (which applies to most of the filings, e.g. change of registered office, directors, shareholders) and GBP 117 (for the late filing of accounts, but only after 2 years of not

⁸⁶ RUBO, Consultation Paper, July 2014.

providing them) and GBP 141,50 (for the late lodging of the annual return, but only after the third year) in the case of not filing changes of information. For the lack of submission, the Registrar has only a faculty to strike off the register the name of any company, other than a public limited company, in respect of which no annual return has been filed in the previous 3 calendar years. Companies may be and are struck off earlier if the Registrar believes a company not to be in operation or carrying on business, as per section 412 of the CompA.

Table 36: Late filing penalties levied by CHG from 1st November 2014 to 11th September 2018

PENALTY TYPE	No. of Penalties	No. of Penalties	No. of Penalties	No. of Penalties
	Nov 2014 - Oct 2015	Nov 2015 - Oct 2016	Nov 2016 - Oct 2017	Nov 2017 - Sept 2018
Late filing of Annual Returns	3305	4116	3730	2465
Late filing of Annual Accounts	3946	4285	4769	3380

525. In addition to striking off a company in respect of which no annual return has been filed in the previous 3 calendar years, the CHG may also strike off any company or limited liability partnership that is believed to be defunct. A relatively large number of companies (11,217 companies in total from the 1st January 2014 to 11th September 2018) have been removed from the Register of Companies over this period. While this shows the capacity of the CHG in detecting instances in which companies are not filing the annual returns or companies that are defunct and of risk-mitigating nature of the measure, this very high number raises concerns related to the potential misuse of non-operational companies.

526. There are no sanctions for providing BO information to the RUBO, within the established deadline (see R.24), which has negative impact on effectiveness as described above.

Overall conclusions on IO.5

527. Gibraltar is rated as having a moderate level of effectiveness for IO.5.

8. INTERNATIONAL COOPERATION

Key Findings

Immediate Outcome 2

- a) Gibraltar has a sound legal framework to exchange information and cooperate with its foreign counterparts in relation to ML, associated predicate offences and FT. Nevertheless, the timeliness of the information exchange is hindered by the shortage in human resources and the lack of clear guidelines in relation to incoming Mutual Legal Assistance (MLA) requests.
- b) Legal assistance has been sought, primarily from the UK and Spain. However, the low number of outgoing requests in the period 2014-2018 raises concerns as to whether Gibraltar authorities proactively seek assistance. Outgoing MLA requests relate primarily to fraud, which does not match with the jurisdiction's risk profile. The indicated delays in receiving replies to requests for assistance and the limited resources that law enforcement agencies have at their disposal to pursue evidence abroad impede their capacity to investigate and disrupt transnational criminal networks involved in ML, drugs trafficking and tobacco smuggling. There have been no outgoing requests related to confiscation during the review period.
- c) Competent authorities engage in all forms of international cooperation, including diagonal cooperation. However, an overall decrease in the number of outgoing requests for information has been observed in recent years. The GFIU rarely seeks information exchange for the purposes of its own analysis. The GGC exchanges information primarily with its UK counterpart.
- d) The assistance provided by the GFIU, including spontaneous information exchange and timeliness of its responses has generally been commended by the global network. LEAs are active in the sphere of formal and informal cooperation using direct communication (police to police, customs cooperation), via liaison officers, Interpol, CARIN and other cooperation platforms. Supervisors reply to requests for information from foreign counterparts, although limited statistics were made available.
- e) Competent authorities exchange basic and BO information on legal persons. Although the assessment team did not identify any particular legal impediment in providing this type of assistance, the deficiencies noted under IO 5 may limit its scope.

Recommended Actions

Immediate Outcome 2

- a) Given the number of different legal acts and conditions regulating the provision of MLA in Gibraltar, authorities should take steps to simplify the existing legal MLA framework.
- b) The staff dedicated to verification and coordination of incoming and outgoing MLA requests should be sufficiently reinforced.
- c) Guidelines and templates should be issued for the filing of incoming MLA requests. Upon receipt of such requests, the authorities should conduct a first screening to verify, whether the basic conditions for accepting a request are met (proper recipient indicated, certified translation attached etc.). Such a screening will allow requesting authorities to provide necessary information for the execution of requests in a timelier manner.
- d) The authorities should introduce as a policy objective seeking MLA in connection with ML/FT

investigations, mindful of Gibraltar's role as an international financial centre and given that a significant portion of these investigations include international elements. Assistance should be pursued especially in the case of investigations concerning transnational criminal networks involved in ML, drugs trafficking and tobacco smuggling, in line with Gibraltar's risk profile.

e) The Gibraltar competent authorities should take a more proactive approach in seeking other forms of information exchange on the transnational elements of their analyses and investigations for the purpose of domestic proceedings.

f) Additional resources should be sought for the units in competent authorities dedicated to international cooperation to support the number of proactive requests.

528. The relevant Immediate Outcome considered and assessed in this chapter is IO.2. The Recommendations relevant for the assessment of effectiveness under this section are R.36-40.

8.1. Immediate Outcome 2 (International Cooperation)

8.1.1. Providing constructive and timely MLA and extradition

529. Gibraltar has a sound legal framework to exchange information and cooperate with its foreign counterparts in relation to ML, associated predicate offences and FT. Details about the legal and institutional framework, including its complexities and the conditions under which information can be provided, are available under R.37-R40.

530. Different acts may be applied depending on the nature of the request, the underlying criminality and the requesting jurisdiction. The most frequently used instruments are the MLA (INT) and EIO Reg. In practice, Gibraltar authorities have a process to determine the most suitable legal instrument to provide assistance to foreign authorities. No guidelines are however available for requesting authorities to ensure that their requests meet the specific conditions stipulated under of the aforementioned acts. This can lead to a situation where additional information would be necessary. The Gibraltar authorities did indicate that they welcomed and encouraged draft requests to be sent for review before they were issued to ensure beforehand that they met all relevant criteria.

531. The Attorney General (AG) serves as the central authority in Gibraltar responsible for receiving incoming MLA requests in respect of investigation and prosecution of crime, criminal asset tracing, restraint and confiscation, and civil recovery (non-conviction-based confiscation). MLAs concerning social and civil tax aspects are handled by the Commissioner of Income Tax. The Office of Advisory Council (OAC) processes requests on behalf of the AG and cooperates with other Gibraltar authorities to ensure their execution. Requests under the European Freezing and Confiscation Orders (EFCO) Reg. were coordinated by the Office of Criminal Prosecutions and Litigation (OCP&L) until October 2018, and thereafter by OAC. Gibraltar authorities plan to move the tasks associated with the processing of incoming MLA requests to the OCP&L in the near future.

532. Gibraltar has witnessed an increase in the number of incoming MLA requests over the last three years. The requests reflect a broad spectrum of offences, but by far the largest number of requests, relate to fraud. Other often indicated offences are drug trafficking, ML and computer fraud and corruption. In case of requests for evidence, the top three sectors providing such information are 1) pre-paid card providers, 2) online gaming operators and 3) banks.

Table 37: MLA requests received

Nature of assistance requested	2014	2015	2016	2017	2018	2019 (I-IV)
Total number of MLA requests	69	55	35	52	75	29
Documentary evidence (e.g. banking and business records)	X	X	25	42	58	23
Witness statements/ Interviews (e.g. Defendant interviews)	X	X	1	4	11	4
Restraint*	X	1	1***	0	2***	0
Confiscation	X	X	0	0	1	0
Videolink	X	X	1	0	1	0
Service	X	X	2	1	1	1
Other	X	X	5	4	4	1
ML related MLA requests**	15	20	10	22	32	13

** Includes requests which are ML only and those which are ML related but have previously been recorded by predicate offence.

*** 1 request - no assets located in Gibraltar, 1 request - defective.

x - No statistical data available.

* During the reporting a further 3 requests for restraint under the EFCO Reg. were received.

533. The aforementioned statistics refer to criminal requests. Gibraltar authorities have also provided available statistics on civil requests – 15 requests in 2016, 14 in 2017 and 9 in 2018.

Timeliness

534. Apart from European Investigation Orders (EIOs), there are no formal rules with regards to the timeframes within which MLA requests should be executed. The OAC records incoming requests and oversees their execution. It has a process for prioritising incoming requests, on the basis of i.a. the criminality (FT), seriousness of the offence, danger of evidence being destroyed and time limitations (trial dates, bail deadlines, action days etc.). The RGP, which is the primary authority responsible for the executing of requests, also has a similar standard operating procedure for processing and prioritisation.

535. The authorities have made statistics available regarding the response times for incoming MLA requests.

Table 38: Timeliness of MLA responses

	2014	2015	2016	2017	2018
Average time to execute incoming MLAs	92 days	82 days	74.5 days	157 days	141 days

536. Although the authorities have recently taken steps to improve their response times, the timeliness of information exchange is hindered by a number of specific factors. In particular, there are limited human resources for validating and executing requests. The OAC has only one dedicated person for handling both incoming and outgoing MLAs and the RGP relies on additional part-time civilian staff⁸⁷ to assist in executing such requests. The response time is also impacted by the lack of guidelines and templates for filing requests to Gibraltar, which leads to a situation where several requests must be supplemented or corrected. Another aspect to be taken into account is the communication through the “Post Box” based in London. Although Gibraltar

⁸⁷ MLA incoming/outgoing requests have moved to OCP&L, at a time after the onsite visit, where two additional retired experienced police officers now handle such requests.

encourages and welcomes direct transmission and communication of MLA requests, in around 33% of cases the correspondence is still conducted via a UK intermediary, resulting into the lengthening of response times. Finally, changes in both the EU and Gibraltar legislation have resulted in changes which temporarily led to delays (e.g. the entry into force of the EIO Directive and the MLA (miscellaneous)). Nevertheless, Gibraltar authorities have also presented cases of urgent requests, where assistance was provided within a few days. In addition, the OAC has presented a feedback summary from the requesting authorities (responses were received for 25% of MLA requests executed in 2018) indicating a 100% satisfaction rate concerning the timeliness of execution, usefulness of contact and on the information/ evidence being what was required.

BOX 20 – CASE STUDY

The Finnish Customs issued an urgent request for assistance on 18 August 2017 which was received on the 12 September 2017 in connection with an investigation related to drugs trafficking and ML. The request was sent using the Post-Boxing arrangements. The evidence was required by the 21 September 2017.

The case related to the selling of narcotics on the dark web, totalling at least EUR 50.000 between January and July 2017. It was found that the suspect had two pre-paid cards and information on these was sought, balances, transactions and any available customer details.

The request was processed by the OAC under the Drug Trafficking Offence Act (DTOA) on the same day it was received and sent to the Central Authority for the issue of a Notice of Nomination for the evidence to be taken in Court.

Evidence was provided on 19 September 2017, a week after its receipt following its execution by the RGP’s ECU. One of the cards was not active and as such had not been used and the other had been loaded with EUR 930.06 and the majority of the monies were subsequently withdrawn in cash at ATMs in four transactions.

537. According to the statistics provided to assessors, in the period between 2016 and 2018 around 15% of MLAs received were refused. In 2018, the refusal rate rose up to 19%, as a result of letters of request (LoRs) received from EU member-states which, at the time, had not transposed the EIO Directive within the scheduled timeframe. The main reasons for refusing to provide assistance are: the absence of reciprocity declaration; missing information in requests; non-certified translation; the referred person or company are not in Gibraltar; fishing; the offence in question was not identified as a relevant offence. The Authorities have provided examples of liaising with requesting countries, indicating the requirements or additional information necessary in order to be able to process such requests.

Table 39: Number of MLAs refused

	2014	2015	2016	2017	2018
Number of MLAs refused	4	9	9	11	15

Extradition

538. Annually, Gibraltar receives a small number of requests for extradition, most of which come from EU member-states (89%). During the reporting period Gibraltar received 18 extradition requests in total, 13 of which were executed (72%). In the same period, 6 more requests were received, but they were later cancelled by the requesting countries (e.g. often the referred person is arrested in their territory).

539. The vast majority of extradition requests are executed under the European Arrest Warrant Act (EAWA). In the case of non-EU countries, the 1870 Extradition Act or the 2002 Fugitive Offenders Act (accessed via the TOCA) are applied, resulting in limitations on the extent of assistance Gibraltar could provide. Despite these complexities, Gibraltar executed such a request submitted by Norway in 2017. The limitations in executing extradition requests from non-EU

countries were recently mitigated with the introduction of the 2018 Extradition Act. Overall, deficiencies in the warrant can inevitably result in the non-execution of a request.

540. The authority responsible for extradition requests is the Governor, but his powers are delegated to the Chief Secretary as long as the matter does not affect the internal security or defence. Once received, the request is reviewed by the OAC to ensure that it meets the relevant statutory requirements. Extradition requests meeting the requirements are forwarded to the Governor (provided that they have not already been received by him). For those requests meeting the statutory requirements, the Chief Secretary directs the Commissioner of Police to execute the warrant.

Table 40: Extradition requests⁸⁸

	2014	2015	2016	2017	2018
Total requests received (EAW's unless indicated)	3	7	0	6 (1 non-EU)	2 (1 non-EU)
Executed	3	6	0	2	1
Not executed	0	0	0	1	1
Refused	0	1	0	2	0

BOX 21 – CASE STUDIES

(Extradition to Norway under the Extradition Act 1870 – Child Abduction)

As a result of a hit on the Interpol only minutes after the notice was uploaded, a wanted person, together with an abducted child was stopped by BCA officers, at the Gibraltar International Airport before he boarded a flight to Morocco on the 16 March 2017. BCA officers then informed GCID of the hit on the Interpol system and subsequently the Norwegian authorities confirmed that the notice was in relation to the child and that the person (father) was wanted for child abduction. As a result, RGP officers detained the person who was taken to Police HQ where he was kept in custody pending further documentation from Norway.

On the 17 March 2017 a provisional request for arrest was transmitted pending the issue of an International Arrest warrant. This was issued and subsequently received.

The person wanted appeared in the Magistrates’ Court for the first time on 20 March 2017. GCID coordinated the international logistics with the OAC and the Norwegian authorities. The RGP conducted the extradition with their Norwegian counterparts.

The child was taken into Care and placed with foster parents for a short time until arrangements were agreed to return it to its mother in Norway.

The wanted person’s surrender was ordered on 10 April 2017, resulting to his surrender on 25 April 2017.

CASE STUDY

Extensive assistance was provided to the Dutch authorities, through police to police assistance using CARIN contacts and culminating in the issue of an EIO and a visit to Gibraltar for the Action Day. The EIO was received on 19 January 2018 and recognised on 31 January 2018, whereas the Action Day took place on 6 March 2018 as originally planned.

The EIO related to an investigation into offences of ML, forgery and fraud. The suspect had previously been convicted of trafficking of heroin and cocaine and received a long sentence. Shortly after he was released from prison, he proceeded to make a number of large cash deposits and gave accounts to the banks as to the

⁸⁸ Where the person has not been located in Gibraltar, the request has not been counted for the purpose of the above statistics (throughout the reporting period there have been 3 such cases).

provenance of the money, which investigators believed to be false.

Extensive assistance was sought which included information from TCSP's, banks, tax authorities, Yacht and Land Registry, trade register, etc. A course of action was agreed with the Dutch Authorities and the execution set for the Action Day.

The Press in the Netherlands reported on the Action Day and the assistance provided in Gibraltar was mentioned.

CASE STUDY - (Operation Ypres)

A request for MLA was received through the OAC by HMC on 17 October 2017 related to an on-going international maritime, drug trafficking case headed by authorities in the UK. The assistance afforded by HMC officers was in the monitoring of individuals, vessels and vehicles. Throughout the operation direct contact was maintained, at ground level, with UK and Spanish LEAs. The MLA requested witness statements from the officers involved, together with data from a local marina and a local telecommunications provider. This material will serve as evidence against those members of the Organised Crime Group who were arrested in relation to the drug trafficking.

Identifying, freezing, seizing and confiscating assets

541. The majority of assistance in connection with the identifying, freezing, seizing and confiscating assets occurs under the EFCO Reg. which transposed the EU Council Framework Decision 2003/577/JHA and 2006/783/JHA. This relates to requests from EU Member States. Other legal instruments such as DTOA and TOCA provide possibilities to provide assistance under specific conditions.

542. Technical limitations in the scope of giving effect to external requests and orders have been recently mitigated with the introduction of the POCA (External Investigations in a Civil Context) Order 2019 and POCA (External Requests and orders) Order 2019. A regime for non-conviction-based confiscation, referred to as "civil recovery", has been recently set out in the POCA (External Investigations in a Civil Context) Order 2019. However, it is too early to determine the effectiveness of the aforementioned legal framework.

543. In situations where the request of assistance cannot be executed under the existing legal framework and the freezing of funds is required, such a request would be forwarded to the GFIU for consideration of a no-consent on the funds, which will allow the freezing of funds.

544. Gibraltar has received four requests for restraint under the EFCO Reg. and 1 request for confiscation. The authorities have provided details of a case study related to funds restraint in 2015.

BOX 22 – CASE STUDY

A request from Portugal dated the 17 February 2015 for the freezing of funds was received by the Senior Crown Counsel at OCP&L on March 4th via the European Judicial Network (EJN). The request concerned a specific sum on an account to be restrained in connection with a fraud and ML investigation. A number of deficiencies were identified in the request. Gibraltar authorities highlighted these deficiencies to the requesting authorities on March 5th, in the meantime the GFIU had placed a "no consent" on the account in question to ensure there was no dissipation of assets.

The additional information necessary to execute the request was provided on 27 March 2015, resulting in the Central Authority sending the request to the Supreme Court for the issue of a freezing order which was duly made on April 2, 2015. So far, the funds remain restrained. A request for confiscation request is yet to be made by the requesting authorities.

8.1.2. Seeking timely legal assistance to pursue domestic ML, associated predicates and FT cases with transnational elements

545. The Gibraltar authorities do not regularly seek legal assistance for international co-operation to disrupt transnational criminal networks involved in ML, drugs trafficking and tobacco smuggling.

Table 41 –Outgoing MLA requests

	2014	2015	2016	2017	2018
Number of outgoing MLAs	4	7	5	3	4

546. The majority of outgoing MLA requests is associated with fraud, which does not correspond with Gibraltar’s risk profile (focus on tobacco smuggling, drug trafficking). The decision to seek MLA is most often initiated by the RGP. MLA requests are verified and drafted by the OAC. During discussions with the authorities it was acknowledged, that LEAs have been reluctant to pursue evidence internationally when a case can be prosecuted without it. Requesting assistance can lead to difficulties in subsequent trials if persons are unwilling to attend Court from overseas. Limited resources and the long execution time of outgoing MLAs were also indicated as the primary reasons why Gibraltar authorities rarely seek such assistance. The absence of complex ML investigations and prosecutions may also to some extent explain the absence of MLA requests to foreign counterparts in such cases.

BOX 23 – CASE STUDY

An EIO application was granted by the Magistrate’s Court on 15/08/2018 and was submitted to the Spanish Courts. This followed the seizure of EUR 8720 in cash from an individual at the Land Frontier with Spain. This person claimed that the money had been loaned to him by his father. The father appeared at the HMC station with some documents including a bank book. When officers informed him of the approximate amount that had been seized from his son, he walked back into Spain returning later with an entry in his bank book for EUR 8000 dated that same day, saying it proved the withdrawal of the money seized. The EIO will ascertain whether the EUR 8000 withdrawal from the bank occurred after the cash was seized and that it was intended to deceive HMC officers. Should the latter be the case, the father will be arrested for Perverting the Course of Justice and the cash will be forfeited.

547. Gibraltar pursues a small number of extradition requests, most often to Spain and the UK. Upon an outgoing request the RGP will submit a report to the OAC. Should the statutory criteria be met, the OAC will draft the request and make an application in the Magistrates’ Court for its issue to a foreign authority.

Table 42 –Outgoing extradition requests

	2014	2015	2016	2017	2018
Number of outgoing extradition requests	1	0	1	3	3

BOX 24 – CASE STUDY (Spain)

On the 13 September 2017 a Detective Inspector of the RGP submitted a request for the issue of two EAWs together with a report setting out the facts of the case. The EAWs were drafted by Crown Counsel at the OAC and an application for the issue of the same was filed on the 14 September 2017. On the 15 September 2017 two EAWs were issued in connection with an offence of conspiracy to cause grievous bodily harm with intent. The wanted persons were apprehended in Spain and extradited to Gibraltar on the 9 April 2018. The wanted persons were charged on their return.

One of the individuals has since pleaded guilty to the offence of inflicting grievous bodily harm and was sentenced to 10 years imprisonment.

548. Throughout the reporting period Gibraltar authorities did not request for confiscation of assets in other jurisdictions. This is supported by the shortcomings analysed under IO 7 & IO 8. Gibraltar has however issued six European restraint orders in connection with one case to the UK.

549. The highlighted limited pro-activeness causes concerns as to whether Gibraltar authorities proactively seek MLA, taking into account that a significant portion of ML/FT investigations include international elements. The tendency to focus on domestic aspects instead, it hampers the ability to investigate and prosecute ML/FT, associated predicate offences and secure the proceeds of crime.

550. In general, Gibraltar's MLA requests are duly executed by its partners. A very small number of requests received no formal acknowledgement. However, the vast majority of them are eventually accepted through the support of liaison officers.

8.1.3. Seeking and providing other forms of international cooperation for AML/CFT purposes

RGP

551. The RGP has various channels for cooperation with its foreign partners, namely: CARIN (Informal Asset Recovery Network), Police to Police channels, Interpol requests (via GCID), LEA Liaison Officers (primarily with Spain), Egmont requests (via the GFIU) and SB bilateral partnerships with foreign agencies concerning counter terrorism. The authorities indicated, that in the case of ML, associated predicate offences and FT the channels most often exploited are CARIN and Egmont (through the GFIU).

552. As for outgoing requests, the decision to make a request is a matter for the discretion of each investigating officer and the approval by the officers' Sergeant or the Force Intelligence Unit. Only partial statistics are available on the number of requests sent out by the RGP.

Table 43 –Outgoing RGP requests

Year	RGP Requests sent via CARIN	RGP Requests sent via Liaison Officer with Spain
2014	No data	No data
2015	21	No data
2016	11	106
2017	15	88
2018	18	44

553. An overview of the statistical data available indicates an overall decrease in the number of outgoing requests for information. The authorities explained that this is mostly a result of complex cases managed during the second half of the review period, which consumed a large amount of resources.

554. With regard to requests received the RGP has a prioritisation process to handle urgent cases without delay. No refusals to incoming information requests were acknowledged in the reporting period. The overwhelming majority of requests come from Spain. Gibraltar receives also requests from other countries, primarily the UK and Germany. The response times vary from 14 days (CARIN, police to police) to the same day (liaison officers). The RGP has provided examples of effective cooperation.

BOX 25 – CASE STUDY (Co-operation with Spain)

Between 2016 and 2017 Gibraltar was in communication with the Spanish authorities on an on-going case relating to Tax evasion, Fraud and ML and provided extensive assistance. This contact was initiated by the Spanish Tax authorities directly to the RGP's MLIU. This has led to investigations in both jurisdictions against an individual and a TSCP in Gibraltar.

The case related to the tax and corporate structures created by the Gibraltar TCSP on behalf of the client who the Spanish authorities claimed was resident in Spain and therefore had a tax liability there. The investigation in Gibraltar related to the requirements for the TCSP to make disclosures to the GFU in relation to the activity of its client.

The intelligence obtained through these enquiries led to two incoming MLA requests by the Spanish authorities processed by the OAC. The requests were executed, and the evidence provided has been essential to their prosecution in Spain.

555. As in the case of outgoing requests, not all statistics on received requests are available.

Table 44 – Incoming requests

Year	CARIN	INTERPOL (dealt with by ECU)	POLICE to POLICE (dealt with by ECU)	Liaison Officer with Spain
2014	No data	No data	No data	No data
2015	9	No data	No data	No data
2016	6	2	3	23
2017	17	1	4	37
2018	23	0	25	37

556. Feedback related to the assistance supplied in police to police and CARIN requests is systematically requested as of June 2018. The assessment team was provided with several examples of high satisfaction rating feedback, particularly in terms of the timeframe during which requests are dealt with, whether the contact with Gibraltar is useful and the relevance of the information supplied.

HMC

557. HMC provides constructive information assistance to its overseas partners. Information is exchanged on the basis of a MoU between the HMC and the French Customs Administration, cooperation in Mar/Yacht-Info SOUTH, cooperation with HMRC liaison officers working in the Foreign and Commonwealth Office (FCO) in Madrid and involvement in the Maritime Analysis and Operations Centre (MAOC). Direct contacts with the relevant Spanish authorities (radio, telephone or face-to-face) add to the effectiveness of information exchange. Examples of successful cooperation with its foreign counterparts were provided by HMC.

558. Financial investigations conducted by HMC often relate to cash seizures and begin with requests for respondents' previous convictions, aiming to ascertain any previous bad character.

559. Only partial statistics are available on HMC information exchange.

Table 45 – Incoming and outgoing HMC requests

YEAR	Number of requests received by HMC	Number of outgoing HMC requests
2014	0	6
2015	7	1
2016	13	7
2017	32	35
2018	41	21

560. HMC has a written procedure concerning data sharing. There is however no process envisaged for sharing information with non-EU countries (apart from referring to provisions of the

Data Protection Act).

BOX 26 – CASE STUDY (Vessel ‘Condor of World’)

In the summer of 2015, an individual was rescued from the sea by a commercial ship. The individual claimed that he had been thrown overboard from a vessel under the name of ‘Alpha Omega II’. The incident was reported to the Gibraltar Port Authority (GPA) which in turn referred the matter to the RGP’s Marine Section.

The vessel anchored in Gibraltar in July 2015, where it was searched by RGP and HMC with negative findings. The composition of the crew members together with some suspicious text messages to a third party, were identified by RGP officers. HMC then registered the vessel with both Yacht-Info and MAOC under a ‘Risk’ category. This information was then shared with the Polish authorities via Interpol channels and further intelligence work was coordinated by GCID. The ‘Alpha Omega II’ then sailed to Spain where the Spanish Guardia Civil kept observations and linked it to a Polish OCG. During this time, it changed colour and was renamed ‘Condor of World’. On 13 October 2015 the risk level category of the vessel was raised to ‘Target’.

In August 2016, the vessel sailed to the middle of the Mediterranean Sea, but returned to the same port days later. It was searched by the Guardia Civil with no findings. A week later the vessel repeated the sailing manoeuvres, although this time it sailed towards Italy. The Italian authorities were informed, thus the vessel was intercepted once more. The search revealed 3300 kilos of cannabis on board.

The investigation continued and searches were carried out on several premises and other vessels. 19 persons were arrested. The following items were seized:

- 3300 kilos of cannabis; 1 sailing boat; 3 vehicles; 2 satellite telephones
- High specification electronic equipment; GBP 20,000; Documentary evidence

561. The Gibraltar LEAs advise that it has neither received nor made any request to form or be part of joint investigation teams (JITs) during the reporting period. However, they are considering participation in such a team related to on-going ML investigations (see IO.8).

GCID

562. The GCID regularly provides information to domestic and foreign LEAs or other competent authorities, primarily through the Interpol channel. In the case of incoming requests, the majority of these relate to fraud and drugs trafficking. Outgoing requests concern most often drugs trafficking, arms trafficking and other offences such as fraud, robbery etc. These requests are primarily initiated by Gibraltar LEAs (HMC and RGP).

Table 46 – Incoming and outgoing GCID requests

YEAR	Number of requests received by GCID	Number of outgoing GCID requests
2014	135	15
2015	68	9
2016	116	3
2017	97	5
2018	48	11

GFIU

563. The GFIU is an Egmont Group member (since 2004) and it exchanges information regularly with its foreign counterparts. The GFIU also cooperates with non-counterpart authorities within the framework of diagonal cooperation. The GFIU does not legally require a MoU with other FIUs, although as an Egmont member it has engaged in signing MoUs with 10 other countries which are required by their laws to do so.

564. The GFIU rarely files requests for information to its international counterparts. Figures show a slight downward trend, despite a large increase in the number of analysed reports. In the

majority of cases where the GFIU takes a proactive approach, enquiries are made on behalf of the RGP. This raise concerns in comparison with the large increase of STRs during the reporting period and the transnational nature of the received STRs. The GFIU focuses on providing spontaneous disseminations to other authorities. Statistics concerning information exchange show a reduction in spontaneous information disseminations to foreign FIUs in the period 2017-2018. This trend has been caused by a review of the quality of outgoing information (previously unsolicited information was sent out to foreign partners automatically) and the introduction of a dual reporting mechanism by the gaming industry (e.g. STRs concerning UK nationals would also be sent by REs to the UKFIU).

Table 47 – GFIU outgoing requests and spontaneous disclosures

YEAR	Number of Outgoing requests	Number of Spontaneous disclosures
2014	17	300
2015	6	330
2016	10	333
2017	23	57
2018	7	108

565. With regard to incoming requests for information, the feedback received from the global network confirms in general that co-operation with the GFIU was effective and resulted in quality assistance. During the onsite, the authorities have provided examples of positive feedback from their foreign counterparts. Nevertheless, at least one country shared negative feedback, whereas few jurisdictions indicated long response times in receiving the assistance sought. One country also highlighted, that it did not receive replies to some of its requests. Overall, delegations acknowledged that they receive good quality of spontaneous disclosures from the GFIU. Concerns were raised by a country as to whether the GFIU can obtain bank account information on behalf of a foreign counterpart. This was raised at the on-site and the GFIU demonstrated that bank account information can be obtained on request of a foreign counterpart under the powers conferred by POCA. Refusals occur rarely, in total 3 have been identified – on the basis of requests not written in English and failure to provide additional information.

Table 48 – GFIU incoming requests

YEAR	Number of Incoming requests	Average Response time
2014	232	2-79 days
2015	145	4-96 days
2016	89	4-195 days
2017	124	2-100 days
2018	125	1-28 days

566. The establishment of an International Desk which is managing the information exchange of the GFIU in 2017 allowed to improve the response times in the following years.

BOX 27 – CASE STUDY

In late 2016, the GFIU received a LoR from the Isle of Man asking for assistance with a case concerning theft of cash from an employer. Subject A was a compulsive gambler and drinker and it was believed that some of the funds in question had been used to support his gambling habit with a Gibraltar based gambling company. The subject fled the Isle of Man to the UK. He was apprehended by the UK authorities where he eventually pled guilty to two charges of theft from his employer.

The GFIU retrieved the relevant intelligence from the local gambling company and forwarded it to the Isle of Man via Egmont within a few days after the request was made. The subject has been sentenced to eight months imprisonment for each of the two thefts.

Supervisors

GFSC

567. The GFSC exchanges information primarily on the basis of bilateral and multilateral Memoranda of Understanding (MoUs). The authorities indicated that in 2019 the MoU with the UK Financial Services Authority is used on average on a weekly or biweekly basis for issues related to firms with the UK. In addition, there are MoUs in place with Malta, Jersey and Guernsey which are utilised frequently for Regulator to Regulator Fit and Proper requests of information, including incoming and outgoing from the GFSC. Should the GFSC wish to disclose certain information to a fellow regulator with whom they do not have a MoU, or where the MoU held does not allow for that specific information to be exchanged, the GFSC may also rely on a further gateway under the FS(IG&C)A (S.3(2)(f)).

568. In October 2018 the GFSC enhanced its procedures on managing requests for information, with a purpose to ensure consistency and efficiency in processing information requests. Among other, this resulted to a centralised register of all requests to ensure that they are adequately logged and tracked.

569. With regard to outgoing information requests, the GFSC confirmed that, 6 requests were sent in the first quarter of 2019. The GFSC has also provided examples of spontaneous disclosures and indicated that the primary recipients are UK authorities. Prior to this period, there were no statistics generated, both for incoming and outgoing requests.

570. The authorities indicated, that in the period between June 2018 and December 2018, the GFSC received 72 requests for information, 74% of which were processed within 1 week (the longest time 41 days). Up to the onsite visit a further 49 requests were received in 2019.

571. The GFSC has provided examples of taking action on the basis of spontaneous disclosures from other authorities and of providing relevant dissemination to the GFIU in cases of potential underlying criminal activity.

BOX 28 – CASE STUDY

Spontaneous intelligence was received from the UK Financial Conduct Authority (FCA) regarding individual A, UK resident, and Company A which was shared on the basis that it made reference to Gibraltar registered companies.

The Gibraltar enforcement team reviewed the intelligence as it concerned possible unlicensed activity in terms of the Company A and Company B. Both companies registered in Gibraltar had issued loan notes, which would potentially constitute investment activities under Schedule 1 (2) of the 1989 Financial Services (Investment and Fiduciary Services) Act. The analysis carried out by the Enforcement team concluded that both companies were carrying on a regulated activity and hence would need to be licensed in line with Section 3(1) of the FS(IFS)A. The analysis and initial investigation made apparent that the unlicensed activity was a potential serious fraud on the part of individual A, through the use of the two (unlicensed) Gibraltar registered companies.

The GFSC assessment indicates that both companies appear to have been set up for the benefit of individual A of Company C, by a UK Independent Financial Advisor. These companies have held investment monies as admitted by Individual A, including UK pension monies, through a self-directed bond administered by a regulated Gibraltar company, of which over 80% is said to be lost / missing with the suspicion that these funds have been spent / misappropriated.

Company C, the UK Independent Financial Advisor, was placed into liquidation on 18 October 2018 and the matter has been reported to the police within the UK (City of London Police and Staffordshire Police). In addition, the FCA investigates Individual A. The case is in the hands of the Enforcement team, albeit in initial

stages.

Given the Enforcement team's concerns in relation to the possibility of fraud, an internal suspicious activity report was submitted to the MLRO. The Enforcement team has been involved in telephone discussions with the FCA, UK LEAs, the UK Sipp Provider and the newly appointed liquidator of Company C as well as the UK Police and National Economic Crime Centre.

Following the latest conversation with the FCA and the UK LEAs, a referral to the RGP will be submitted. The case is still on-going.

572. It is highlighted, that in the reporting period the GFSC has not denied the provision of information. The GFSC does not request nor was ever requested to provide feedback, however it received feedback from the global network is with regard to international cooperation.

GGC

573. The GGC exchanges information with its foreign counterparts mostly in the field of licensing, supervision and reports of systemic failure. Its main partner is the UK Gambling Commission, with which the GGC has signed a MoU.⁸⁹ Although the client base of Gibraltar's gambling operators includes a large number of foreign nationals, the largest proportion of customers are UK residents and therefore cooperation with the UK covers the majority of information exchanges. There are no cases of refusal to information requests from foreign partners. Scarce feedback on the quality of the GGC's responses is received, in most cases, informally from the UK regulator. Apart from responding to information requests of its counterparts, the GGC also assists the RGP in the execution of relevant MLAs in its capacity as a supervisor of the gambling sector.

574. With regard to outgoing requests, most of them are related to regulatory issues. However, disclosures concerning problematic gambling have also been conducted. No formal statistics are held on incoming and outgoing requests.

BOX 29 – CASE STUDY (UK Gambling Commission)

A 2018 case involved the acceleration of a case to the UK Gambling Commission, where open source checks (conducted by the Gambling Division) clearly showed the association of a female subject (based in the UK) with a charitable enterprise supporting the health of a close relation. It was clear that the subject's level of gambling activity and losses could not be supported from her own funds and the case was escalated directly by the Gambling Commissioner to a UK Executive director as the matter required urgent action by way of email in January 2018. Gambling had taken place across more than one operator. The Gambling Division also liaised with the GFIU and confirmed the case had been reported to the National Crime Agency in the UK. There was ultimately a prosecution and conviction in the UK.

575. In addition, cooperation takes place with two US regulators (New Jersey and Nevada) by meeting with and discussing various regulatory matters with said regulators when conducting investigation visits to local operators. There is also on-going cooperation (multi case) on sports betting integrity issues with the UK Authorities and sports governing bodies.

OFT, RSC

576. Both the OFT and the RSC have the power to cooperate with foreign competent authorities. The SBPR (Reg.9) provides the legal basis for such cooperation with EU Member States. The aforementioned authorities did not indicate a framework for cooperation with counterparts from

⁸⁹ The GGC indicated that it is in the process of concluding MoUs with the relevant authorities of Sweden and Malta. The MoU with the Swedish gambling regulator was signed in a time following the on-site visit (8 May 2019).

non-EU jurisdictions. In practice, both competent authorities have not engaged in cooperation with their foreign partners on AML/CFT matters. The authorities explained that the entities supervised by the OFT and RSC are predominantly operating and providing services solely in Gibraltar.

8.1.4. International exchange of basic and beneficial ownership information of legal persons and arrangements

577. Competent authorities such as the RGP, HMC and the GFIU have processes for exchanging basic and BO information on legal persons. In addition, they have direct access to the Companies House Register. LEAs would approach the GFIU to obtain accurate information on the beneficial owner, for instances where an associated natural person is identified as a nominee associated with a TCSP.

578. As indicated under IO 5, Gibraltar has a functioning RUBO. The Finance Centre Director is the Single Point of Contact (SPOC) for foreign ultimate beneficial owner (UBO) information requests from the UK. The United Kingdom LEAs are able to directly request the BO information contained in the register. Upon receipt of such a request the GFIU simultaneously will perform checks on its systems to identify any positive hits which may be of interest to the requesting authorities of the UK. In the event where there is information within the GFIU's databases, such information is supplied to the requesting authority via the Egmont Secure Web (ESW) as a spontaneous disclosure. The Finance Centre Director has received 24 requests from the UK authorities in 2018. Requests from other jurisdictions are processed via the counterpart Gibraltar authority.

579. The OAC has identified 6 incoming MLA requests between 2016 and 2018, which concerned information on beneficial owners. In all cases BO information was provided. A further 4 requests were received in 2019 (till the end of the onsite visit). The execution time of these requests varied significantly, from an average 232 days in 2016 to 25 days in 2018.

BOX 30 – CASE STUDY

In the period 2017-2018 liaison took place between the RGP CARIN and the Dutch Police in an on-going investigation which led to the identification of assets through corporate structures in preparation. Part of the request was information on the BO of the companies from the TCSP. The information provided allowed for a targeted EIO to be issued.

The EIO was executed on the designated Action Day and 2 Dutch officers attended Gibraltar to assist with enquiries and spent several days in Gibraltar working with the RGP.

580. Although the assessment team did not identify any particular legal impediment in providing this type of assistance, the deficiencies noted under IO 5, may have a negative impact on its scope.

Other authorities

581. In the years 2016-2018, Gibraltar has received a total of 209 requests for information concerning fiscal matters from USA, the UK, Spain, Sweden and other EU member states. Since 2015, Gibraltar has been supplying comprehensive tax data on an automatic basis under the Foreign Account Tax Compliance Act (FATCA) to the US. Similarly, Gibraltar uses the UK FATCA Intergovernmental Agreements since 2016 to provide tax data to the UK. In addition, since 2017, Gibraltar exchanges comprehensive tax data on an automatic basis with all EU Member States under the EU version of the Common Reporting Standard, along with the 'first wave' of countries under the Common Reporting Standard. However, during the reporting period, Gibraltar authorities have not sent out any requests for information on fiscal matters to other countries.

Overall conclusions on IO.2

582. **Gibraltar is rated as having a substantial level of effectiveness for IO.2.**

TECHNICAL COMPLIANCE ANNEX

1. This annex provides detailed analysis of the level of compliance with the Financial Action Task Force (FATF) 40 Recommendations in numerical order. It does not include descriptive text on the country situation or risks and is limited to the analysis of technical criteria for each Recommendation. It should be read in conjunction with the Mutual Evaluation Report.

2. Where both the FATF requirements and national laws or regulations remain the same, this report refers to analysis conducted as part of the IMF Assessment in 2007. This report is available from <https://rm.coe.int/gibraltar-detailed-assessment-report-on-anti-money-laundering-and-comb/1680716081>.

Recommendation 1 – Assessing risks and applying a risk-based approach

3. This is a new Recommendation which was not assessed in the first MER of Gibraltar.

Risk assessment

4. **Criterion 1.1** – In addition to a threat matrix developed in 2012, Gibraltar conducted its first National Risk Assessment (NRA) in April 2016 and complemented it with a more detailed jurisdictional assessment of the financing of terrorism (FT) risk in November 2016 and a further FT NRA for the non-profit organisations (NPO) sector. Authorities advised that the methodology used to conduct the NRA was drawn largely on the FATF’s guidance.

5. In September 2018, Gibraltar revised its NRA to bring it in line with the EU Supra-National Risk Assessment (EUSNRA). The 2018 NRA aims at assessing new risks and updates, for products and services, existing threats and vulnerabilities in a Gibraltar context, both for money laundering (ML) and FT, and with the goal of building up on the findings of the 2016 NRA.

6. Despite these commendable efforts, these assessments are not always comprehensive, which affects Gibraltar’s identification and assessment of the ML/TF risk for the jurisdiction. In particular, Gibraltar has not conducted a comprehensive assessment of the threat, particularly the cross-border threat to which it is exposed as an international financial centre. Significant sectors, such as the banking sector and banking products and services, were not included in the 2016 NRA, and where only assessed as products and services by the 2018 NRA, which is a serious shortcoming given the size and materiality of this sector and affects the identification and understanding of the risk for the jurisdiction. In general, the 2018 NRA is based only on products and services without a holistic approach in understanding and assessing the overall risk that the jurisdiction as a whole, may face. This is compounded by an analysis of the vulnerabilities that, at times, is not comprehensive and limited to considering that a given product or service is subject to preventive measures. In some instances, the findings are not consistent with the analysed threat, both in the case of ML and FT.

7. **Criterion 1.2** – Regulation 5 of NCOR assigns the National Co-ordinator (NCO) to take the responsibility to carry out a risk assessment and keep it up to date. In addition, NCO provides advice to HM Government of Gibraltar (HMGoG) on policy and operational matters designed to mitigate the risks identified in producing the risk assessment as well as the legislative and operational framework required to meet international standards.

8. **Criterion 1.3** – The NCOR assigns to the NCO the responsibility to ensure that risk assessment or any subsequent risk assessment is kept up to date (Regulation 5(1), and also R7). Gibraltar conducted its first comprehensive NRA in April 2016, complemented it with a more

detailed assessment of the FT risk in November 2016, and reviewed the NRA in 2018 after the publication of the EUSNRA.

9. **Criterion 1.4** – A redacted version of the 2016 NRA and the full version of the 2018 NRA are publicly available documents⁹⁰ and thus accessible to both public authorities and reporting entities (REs), including through their supervisors. Regulation 7 of the NCOR requires the NCO to submit the review of the risks to the Minister for Financial Services; Regulation 8 requires that the report must be used to make appropriate information available promptly to a relevant financial business⁹¹ (RFB) to facilitate carrying out of their own ML/FT risk assessments. The 2016 and 2018 NRA reports were communicated to stakeholders (authorities and private sector) by email, whereby the finding of the 2016 FT and NPO NRA were shared through outreach programmes to the public and private sectors.

10. **Criterion 1.5** – Following the publication of the 2016 NRA, an action plan was designed and put into effect in December 2016 with specific risk mitigation measures for the risks identified by the April 2016 NRA; however, no specific measures were identified to mitigate the risks acknowledged by the November 2016 FT NRA (except for recommended actions related to the vulnerabilities identified in the 2017 risk assessment of the NPOs) and for some of the new risks identified by the 2018NRA. There is no risk-based allocation of resources for the supervision of lawyers and notaries (although they feature among the highest risks identified by the 2018NRA).

11. In April 2017 Gibraltar adopted an AML/CFT strategy that outlines the high-level strategic outcomes (prevention, detection, enforcement, international and awareness), with specific actions for attaining them. In January 2019, an action plan was also adopted to follow up on the findings of the 2018 NRA. Regulation 8 of the NCOR requires that the NRA report must be used to assist in the allocation and prioritisation of resources to combat ML and FT. The 2017 Strategy requires Heads of Department, CEOs and senior management of each Authority to ensure that the action plans deliver the required mitigation within acceptable timeframes and that the necessary resources are applied and prioritised. The strategy acknowledges that an effective mechanism for risk profiling regulated firms and their sector is pivotal in the dedication of resources by the supervisors. The 2016 action plan includes measures aimed at the more effective use of resources based on risk (e.g. for the Gibraltar Financial Services Commission (GFSC) to enhance the risk-based approach (RBA) supervision and the GCID to focus resources on high-risk individuals involved in organised crime). Following the 2016 NRA resources were increased for the GFIU and the Gibraltar Royal Police (RGP).

12. **Criterion 1.6** – There are a number of exemptions in the AML/CFT Guidance Notes. Firms are not required to verify identity in the case of public listed companies admitted to trading on a regulated market within the meaning of Directive 2014/65/EU in one or more Member States and listed companies from third countries which are subject to disclosure requirements consistent with Community legislation (6.2.1.2.1., in these cases FATF only exempts from the verification of the shareholders or beneficial owner' identity, not of the company's) or when there are reasonable grounds for believing that the applicant for business is itself a financial institution in Gibraltar or an EU country (6.2.1.2.2). The GFSC AML/CFT Guidance Notes (7.2.2.) also exempt verification in "exceptional circumstances", when applicants for business will not be able to provide appropriate documentary evidence of their identity and where independent address verification is impossible. In such cases, firms might agree that a senior manager may authorise the business if he/she is satisfied as to the applicant's acceptability. Moreover, the record keeping requirements do not

⁹⁰https://www.gibraltar.gov.gi/new/sites/default/files/HMGoG_Documents/NationalRiskAssessment2016-04-PUBLIC.pdf

⁹¹ 'financial businesses' is defined by S.9(1) of the POCA and includes financial institutions and DNFBPs.

expressly apply to the beneficial owner, only the customer, as noted under the analysis of R10. In case of SDD, RSC Guidance mentions that a legal professional is not required to obtain information on the nature and purpose of the business relationship or on beneficial owners, and it is implied that neither on-going monitoring is not required. The definition of beneficial owner adopted by the GFSC GN in the case of trusts limits it, in the case of beneficiaries, to those that own 25% or more of the assets within the trusts. There are blanket exemptions from the application of correspondent banking requirements in the case of FIs based in the EEA. These exceptions and non-application of FATF requirements are not based on verified low risk and are not in line with the FATF R10.

13. **Criterion 1.7** – POCA (S17) provides for enhanced customer due diligence (ECDD) measures mirroring the provisions of the 4th Money Laundering Directive (4MLD) as to specific instances where EDD must be conducted (Correspondent Banking, Non-face to face relationships, PEPs,) as well for any other category which the Minister may designate by Notice, or when a RFB has itself found to be of high risk. Regulation 8 (a) of the NCOR states that the NRA report must be used to improve the AML/CFT regime, in particular by identifying any areas where a RFB is to apply enhanced measures, and where appropriate, specifying the measures to be taken. Although the NRA identifies specific high-risk areas for ML (e.g. tax planning structures and transactions; real estate, securities and funds sector) and FT (e.g. virtual currencies and pre-paid cards) no other higher risk scenarios subject to ECDD (as per POCA S.17) have been designated by the Minister. S.25A of POCA requires financial businesses to take appropriate steps to identify and assess the risks of ML/FT, taking into account risk factors including those in relation to their customers, countries or geographic areas, products, services, transactions or delivery channels, and any information that is made available to the RFB pursuant to the NCOR; but no specific information for applying EDD in higher risk scenarios (e.g. those identified by the NRA) was provided pursuant to the NCOR.

14. While S.25A of POCA requires financial businesses to take appropriate steps to identify and assess the risks of ML/FT, taking into account, inter alia, “any information that is made available to the RFB pursuant to the NCOR”, this is not the same as ensuring that information on higher risks identified by the jurisdiction is actually incorporated in the firms’ risk assessments.

15. **Criterion 1.8** – Simplified due diligence is allowed by S.16 of the POCA when the financial business identifies areas of lower risk. However, it is left to the discretion of financial businesses to determine the circumstances under which a simplified CDD can be applied. Although these should be underpinned by the firms’ assessment of risk, there is no requirement that such assessment needs to be consistent with the jurisdiction’s assessment of the ML/FT risks. S16 (3) of POCA requires a RFB to take into account at least the factors of potentially lower risk situations set out in Schedule 6 of the POCA, but those factors are not based on an actual assessment of risk. When applying SDD lawyers are exempted from identifying the BO.

16. **Criterion 1.9** – Supervisors and SRBs are required to ensure that financial institutions (FIs) and designated non-financial businesses and professions (DNFBPs) are implementing their obligations under R.1. See analysis of R. 26 and R. 28 for more information.

17. **Criterion 1.10** – Section 25A of the POCA requires a RFB to take appropriate steps to identify and assess the risks of ML/FT, taking into account risk factors including those relating to their customers, countries or geographic areas, products, services, transactions or delivery channels, and any information that is made available to the RFB pursuant to the NCOR. This requirement can be waived by a competent authority, which may decide that individual documented risk assessments are not required where the specific risks inherent to the sector are clear and understood. When the competent authority takes such a decision it shall ensure that the

RFBs which it supervises are informed accordingly. No such decision has been taken by the supervisory bodies.

18. Section 25A of the POCA requires financial business to:

- a) document their risk assessment (S25A(3) of POCA);
- b) Take appropriate steps to identify and assess the risks of ML/FT, taking into account risk factors including those related to their customers, countries or geographic areas, products, services, transactions or delivery channels, and any information that is made available to the RFBs pursuant to the NCOR (S.25A(1) of the POCA) and establish and maintain appropriate and risk-sensitive policies, controls and procedures (S.26 of the POCA)
- c) keep these assessments up to date (S.25A(3) of the POCA);
- d) S.25A(3) of the POCA requires RFBs to make their risk assessment available to the competent authorities.

19. **Criterion 1.11** –

a) Section 26 of the POCA requires a RFBs to maintain appropriate and risk-sensitive policies, controls and procedures, proportionate to its nature and size, relating to, inter alia, risk assessment and management. Pursuant to S.26A such policies, controls and procedures must be approved by senior management.

b) For entities supervised by the GFSC, Chapter 5(3) - Recommendation 9 of the AMLCFTGN requires firms to carry out regular assessments of the adequacy of their systems and controls to ensure that they manage the ML/FT risk effectively. For all types of REs POCA (S. 26.1.A) only requires a RFB, where appropriate and bearing in mind the size and nature of the business, to undertake an independent audit function for the purposes of testing the policies, controls and procedures. This requirement however does not fulfil this sub-criterion - it is rather relevant for C.18.1(b).

c) S.17(1)c(i) and (ii) of the POCA requires a RFB to conduct enhanced due diligence measures to appropriately manage and mitigate risks where a financial business itself has identified cases of higher risk (or if the risks were identified by the Minister with notice in the gazette).

20. **Criterion 1.12** – S.16(1) of the POCA allows a financial institution or DNFBP to apply simplified measures if lower risks are identified. There is no specific provision prohibiting simplified due diligence whenever there is a suspicion of ML, but s 16 provides that the application of simplified measures cannot derogate from the need to undertake sufficient monitoring of the transactions and business relationships to enable the detection of unusual or suspicious transactions. S11(1)(c) of POCA requires CDD measures to be conducted if a RFB suspects ML/FT regardless of any derogation, exemption or threshold.

Weighting and Conclusion

21. Gibraltar has undertaken several assessments of the ML and FT risks, with some credible results. However, the identification and assessment of the ML/TF risk of the jurisdiction is not comprehensive; there are exemptions to the application of CDD and record keeping requirements that are applicable to all types of REs and are not based on a proven low risk; simplified due diligence and enhanced due diligence are not based on the higher/lower risks identified by the jurisdiction. **R.1 is rated Partially Compliant (PC).**

Recommendation 2 - National Cooperation and Coordination

22. In its first MER, Gibraltar was rated LC on R31. The MER noted that the DNFBP oversight authority (excluding GFSC respect to TCSPs) is not represented in the Enforcement Group. As the requirements in Recommendation 2 have changed considerably since then, the 1st MER analysis is no longer relevant.

23. **Criterion 2.1** – In April 2017 Gibraltar adopted an AML/CFT strategy that outlines the high-level strategic outcomes (prevention, detection, enforcement, international and awareness), with specific actions for attaining them. The strategy is informed by the risks identified by the 2016 NRA, as well as by the FT risks identified by the FT and NPO risk assessments. There are no immediate plans to revise the strategy in light of the revised NRA: authorities reviewed the current Strategy and resulting action points and are of the view that a revision of the strategy is not required, as it remains relevant. However the full relevancy of the 2017 strategy can be questioned, given the increase in the risk identified in certain areas between the 2016 and the 2018 NRAs (for example the proximity to organised crime) and the fact that new risks were identified, which were not identified in the 2016 NRA (e.g. the use of products in the banking sector, cash intensive businesses and international sanctions).

24. **Criterion 2.2** – There is no formal designation of an authority, but there is a mechanism envisaged for national AML/CFT policy. Regulation 4 of the NCOR provides that the national coordinator responsibility is in charge of giving advice on ‘policy and operational matters designed to mitigate the risks, identified in producing the risk assessment.’ The advice on the risks identified must be provided in the form of policy and guidance notes and must be based on current information and be kept up to date (NCOR Regulation 5(3)). In other words, his/her role is limited to risk assessment only and does not concern overall national. The 2017 Strategy acknowledges the NOC’s role to ensure a strategic and proactive approach to the development of policy, legislative as well as workflows to improve the AML/CFT regime. In order to provide a more formalised support for the NCO, the strategy had also envisaged that HMGoG would have established a formal Steering Committee structure where all policy, legislative and workflows will be discussed, and recommendations made to HMGoG for their attention and action as necessary. However, the Steering Committee was not in place at the time of the onsite visit.

25. **Criterion 2.3** – At an operational level there is an Interagency Working Group which meets every two months to discuss operational matters. The Interagency Working Group consists of the following stakeholder authorities: GFSC, RGP, GLO, GFIU (and GCID), HMC, ITO, OFT, GC, GCS. The Group discusses, as per ToRs, matters of mutual interest that impact or could potentially impact the Financial Services industry and the reputation of Gibraltar, including: i) Financial Crime Trends; ii) Operational Challenges; iii) Deficiencies in the current Law; iv) Moneyval and any other evaluations; v) The best use of resources; vi) On-going investigations; and vii) Training. At policy level the mechanism in place consists of meetings of the NCO with the Minister at regular intervals (once every two months) and with stakeholder authorities to review operational plans as well as any proposals for development of specific policies and attainment of action plan items (every 8 months).

26. **Criterion 2.4** – There exists no separate coordination mechanism for PF. Authorities stated that the same mechanism as for AML/CFT would apply, as a result of October 2018 meeting in which proliferation financing has been added as a standing agenda item for the inter-agency working group.

27. **Criterion 2.5** – Gibraltar has transposed the EU Data Protection Directive Directives (EU) 2016/680 and 95/46/EC Directive (EU) 2016/680 through the Data Protection Act 2004 (as amended) as well as GDPR Regulation (EU) 2016/679. This affords the necessary protections

regarding the privacy and exchange of information as well as the use of information obtained or processed. The inclusion of a specific Section in POCA (S34A) ensures the compatibility between the AML/CFT legislation and the data protection legislation (the Data Protection Act and GDPR) by providing specific referencing to data subject rights, the processing by RFBs for ML and FT prevention, disclosure to clients of data protection provisions and prevention of tipping off, etc due to a data access request. The Data Protection Commissioner of Gibraltar makes himself available to both authorities and RFBs should there be a need to clarify the workings or interpretation of legal provisions that apply. The Data Protection Commissioner also took part in the 2016 NRA process exactly for these same reasons. Although there are no formal mechanisms established for these purposes, access to the Data Protection Commissioner and his staff is easily obtained by public and private sector bodies.

Weighting and Conclusion

28. Gibraltar has mechanisms through which national co-operation and coordination can be achieved and has a strategy that is mostly informed by the risks identified. However, the full relevancy and up-to-datedness of the 2017 strategy can be questioned, given the increase in the risk identified in certain areas between the 2016 and the 2018 NRAs (for example the proximity to organised crime) and the fact that new risks were identified, which were not identified in the 2016 NRA. **R.2 is rated Largely Compliant (LC).**

Recommendation 3 - Money laundering offence

29. In the 2007 IMF Report, Gibraltar was rated partially compliant. The ML offence was found in both the Criminal Justice Ordinance 1995 (CJO) and the Drug Trafficking Offences Ordinance 1995 (DTOO) giving rise to a need for prosecutors to prove whether the property, which was the subject of the charge, was the proceeds of criminal conduct (excluding drug trafficking) or of drug trafficking. At the time of the 2007 Report trafficking in human beings and migrant smuggling (section 63A of the Immigration Control Ordinance; sections 62-65 of the Immigration Control Ordinance) were ‘summary offences’⁹² only and thus not predicate offences for ML. Failure to obtain a licence for the export of cigarettes under the then Tobacco Ordinance 1997 was also a summary offence and therefore not a predicate offence for ML.

30. **Criterion 3.1** – CJO has been replaced by the Crime (ML and Proceeds) Act of 2007 which itself has been superseded by the Proceeds of Crime Act (POCA) 2015 (in force since 28th January 2016). The current statutory framework for criminalisation of ML in Gibraltar is contained in the POCA 2015 which reformed the criminal law with regard to ML by replacing separate drug trafficking and criminal justice legislation with a consolidated and updated set of provisions. Gibraltar has three substantive or principal ML offences in the POCA which criminalise ML as required by the Palermo and Vienna Conventions and as follows:

Arrangements: where a person enters into or becomes concerned in an arrangement which he/she knows or suspects will facilitate another person to acquire, retain, use or control criminal property (s. 2)

Acquisition, use and possession of criminal property: where a person acquires, uses or possesses criminal property (s. 3).

⁹² “summary offence” means an offence which if committed by an adult is not triable on indictment except in conjunction with an indictable offence; an “indictable offence” means an offence which if committed by an adult is triable on indictment, whether or not it is also triable by the Magistrates’ Court (S.2 of Criminal Procedure and Evidence Act).

Concealing etc.: where a person conceals, disguises, converts, transfers or removes from Gibraltar any criminal property (s.4).

31. **Criterion 3.2**– The ML offences are defined in relation to criminal property constituting or representing the benefit from criminal conduct (s.182 (1A)). This covers all “criminal conduct” which if it occurs in Gibraltar would be an offence in Gibraltar; or which if it did not occur in Gibraltar would constitute an indictable offence in Gibraltar if it occurred there (s. 182).

32. **Criterion 3.3** – Rather than applying an “all crimes” approach, Gibraltar applies a combined approach which includes a threshold approach. All offences committed in Gibraltar are predicate offences for the money-laundering offences set out in section 2, 3 and 4 of POCA. Any offence committed outside of Gibraltar is a predicate offence for the money-laundering offences provided that it would be an indictable offence in Gibraltar if it had occurred there. Under section 2 of the Criminal Procedure and Evidence Act 2011, an indictable offence is defined as an offence which if committed by an adult is triable on indictment, whether or not it is also triable by the Magistrates’ Court. There are criminal offences in Gibraltar which are not indictable but are summary only offences. These are less serious criminal offences where the maximum sentence is less than one-year imprisonment. The vast majority of the main predicate offences for the money-laundering offences in Gibraltar are indictable. The proceeds of foreign predicate criminality in all serious cases would therefore be criminal property and the laundering of these proceeds would be criminalised in Gibraltar. All designated categories of offences are covered under Gibraltar law. Tax Crimes are also covered.

33. **Criterion 3.4** – The ML offences extend to any type of property of any value. “Criminal property” is a) the benefit from criminal conduct or representing such benefit (in whole or part and whether directly or indirectly) and b) the offender knows or suspects that it constitutes or represents such a benefit (POCA s. 182 (1A)). The definition of property is wide, meaning “assets of any kind, whether corporeal or incorporeal, moveable or immovable, tangible or intangible and legal documents or instruments in any form evidencing title to or an interest in such assets” (s. 183(1) POCA.) The definition of criminal property in the POCA is not limited to property in Gibraltar and therefore covers property wherever it is situated.

34. **Criterion 3.5** – The ML offence does not require that someone be convicted of the predicate offence and neither the specific nor even the type of predicate offence needs to have been identified to prove ML. There are no legislative barriers to autonomous ML prosecutions and convictions. It is necessary to prove, beyond reasonable doubt, that the property constitutes or represents the proceeds of crime and that the defendant committed the alleged ML offence (POCA Ss. 2-4; 182-183). Case law⁹³ from the Court of Appeal of England and Wales also confirms that prosecutors are not required to prove that the property in question is the benefit of a particular or a specific act of criminal conduct, as such an interpretation would restrict the operation of the legislation. The prosecution needs to be in a position, as a minimum, to be able to produce sufficient circumstantial evidence or other evidence from which inferences can be drawn to the required criminal standard that the property in question has a criminal origin. In other words, the prosecution must simply lead enough evidence so that the jury can draw an inference that the property concerned is “criminal property”.

⁹³ *Anwoir, Elmoghrabi, Meghrabi, McIntosh* [2008] EWCA Crim 1354, Court of Appeal Decision (The decisions of the Court of Appeal and the Supreme Court (formerly the House of Lords) of England and Wales are persuasive authority in Gibraltar. Section 2 of the English Law (Application) Act (<https://www.gibraltarlaws.gov.gi/articles/1962-08o.pdf>) is the authority that provides that common law and the rules of equity from time to time in force in England shall be in force in Gibraltar, so far as they may be applicable to the circumstances of Gibraltar and subject to such modifications thereto as such circumstances may require.)

35. **Criterion 3.6** – Any offence committed in Gibraltar or criminal conduct if it does not occur in Gibraltar and would constitute an indictable offence in Gibraltar if it occurred there, is a predicate offence for ML (POCA s.182). There is no foreign legality exclusion. Conduct which would be indictable in Gibraltar if it had occurred there can be a predicate offence for the ML offences even if not constituting a criminal offence in the jurisdiction outside Gibraltar.

36. **Criterion 3.7** – The ML offences of acquisition, use and possession of criminal property (POCA s. 3) and of concealing, disguising, converting, transferring or removing from Gibraltar any criminal property (POCA s.4) may be committed by a predicate offender or a third party. Arrangements under POCA s. 2 apply to a person who enters into an arrangement with the predicate offender. For the ML offences, it is “immaterial who carried out the [predicate offence]” (POCA s. 182(5).)

37. **Criterion 3.8** – A ML offence is committed where the property constitutes a person’s benefit from criminal conduct and the accused knows or suspects that it does. It is a principle at common law that reasonable inferences may be drawn from objective factual circumstances. Section 4 of the Crimes Act states that the court or jury (i) is not bound in law to infer that the person intended or foresaw a result of his actions by reason only of its being a natural and probable consequence of those actions; but (ii) must decide whether he did intend or foresee that result by reference to all the evidence, drawing such inferences from the evidence as appear proper in the circumstances. There are two ways in which the Prosecution may prove the property derives from criminal conduct: a) by showing that it derives from conduct of a specific kind or kinds and that conduct is unlawful, or b) by evidence of the circumstances in which the property is handled which are such as to give rise to the irresistible inference that it can only be derived from crime (*Anwoir, Elmoghrabi, Meghrabi, McIntosh* [2008] EWCA Crim 1354).

38. **Criterion 3.9** – Proportionate and dissuasive criminal sanctions apply to natural persons convicted of ML. The ML offences are punishable on indictment by up to 14 years imprisonment, a fine or both. The level of fine is unlimited and there is no minimum level of fine for ML offences.

39. **Criterion 3.10** – Criminal liability and sanctions apply to legal persons, without prejudice to the criminal liability of natural persons. Legal persons are punishable by a fine. Criminal liability and sanctions apply to legal persons by virtue of s.2 of the Interpretation and General Clauses Act 1962 which includes within the ambit of “person” any corporation either aggregate or sole, and any club, society or other body. Corporate criminal liability does not prejudice the criminal liability of a natural person (s.34 POCA.) Under S.69 of POCA civil recovery regime can be applied to property obtained through unlawful conduct by legal entities. S.184 of POCA provides for subsidiary legislation giving under the Supervisory Bodies (Powers etc.) Regulations 2017 enforcement and sanctioning powers.

40. **Criterion 3.11**– The interpretation section of Part II POCA headed “Money laundering and other offences” has no definition of ML. It is recommended that POCA explicitly extends the definition of ML at Part III so that it also defines ML for Part II and Part VI. The interpretation section of Part III headed “Measures to prevent the use of the financial system for purposes of ML and terrorist financing” at 7(2) extends the definition of ML to include any FT offences.

41. Whilst attempts, inchoate offences and conspiracy in relation to the ML offences (s.2, 3 and 4 of the POCA) are not explicitly covered in POCA, other legislation covers the attempts to commit an offence (s. 22 Crimes Act 2011); a conspiracy to commit an offence (s. 27 Crimes Act 2011); a conspiracy to commit an offence outside Gibraltar (s.28 Crimes Act 2011); aiding and abetting the commission of an offence (s. 47 CA 2011); encouraging or assisting the commission of an offence (ss. 36 and 37 Crimes Act 2011).

42. The specific ML offence applies to those who enter into or become concerned in an arrangement which will facilitate ML (s. 2 POCA).

Weighting and Conclusion

43. All criteria are met. **R.3 is rated compliant (C).**

Recommendation 4 - Confiscation and provisional measures

44. In the 2007 IMF Report, Gibraltar was rated largely compliant with the then R.3 of the FATF. The authorities' power to seize suspect cash at the border was limited in non-drug related cases and the post-conviction burden to show that proceeds were legitimate shifted only in drug-related cases as well.

45. **Criterion 4.1**– The legal framework enabling the restraint and confiscation in Gibraltar is covered in the POCA and in the Terrorism Act 2018. POCA replaced and consolidated separate drug trafficking and criminal justice legislation.

a) With respect to the laundered property, Part IV of POCA deals with the confiscation of the proceeds of criminal conduct and s. 35 provides for post-conviction confiscation orders. The Attorney General also has powers to pursue the civil recovery of the proceeds of unlawful conduct pursuant to Part V of POCA without the need for a conviction. Cash seizures: (s. 119 POCA) cash in excess of GBP 1,000 may be seized if it is recoverable property (s.70 POCA) or intended by any person for use in unlawful conduct.

b) The assessment of the proceeds of criminal conduct is governed by s. 37 POCA. The confiscation regime is value based. A s. 35 confiscation order is an order made against the person not the property. The proceeds of a person's criminal conduct are "any payment or other rewards received by a person at any time in connection with criminal conduct carried on by him or another person." In determining whether a defendant has benefitted from criminal conduct in respect of any ML offence or any predicate offence statutory assumptions are made (unless they are shown to be incorrect) such as that any item of property transferred to him in the 6 years preceding the institution of proceedings against him was payment or reward in connection with the criminal conduct carried on by him.

S. 604 of the Criminal Procedure and Evidence Act (CPEA) 2011 provides a power of forfeiture when a person is convicted of an offence and the court 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 has been used for the purpose of committing, or facilitating the commission of, any offence; or was intended by him to be used for that purpose, the court may make a forfeiture order in respect of that property.

c) Property used or intended for use in terrorism offences or that was received as payment or reward for terrorism offences can be confiscated under the usual criminal or civil regimes. The FT offences (ss. 35-39 Terrorism Act 2018) are indictable offences and may therefore be the subject of post-conviction confiscation orders under s. 35 POCA 2015. Forfeiture of property may also be achieved from individuals convicted of a relevant terrorism related offence: s. 56 Terrorism Act 2018 covers forfeiture in connection with the FT offences; s. 57 Terrorism Act 2018 covers forfeiture in connection with other terrorism offences and offences with a terrorist connection. Cash may also be forfeited in civil proceedings if it was intended for FT, represents the assets of a proscribed organisation, or is or represents property obtained through terrorism (s. 62 Terrorism Act 2018).

d) Confiscation under POCA 2015 is based on value. The court determines whether the defendant has benefited from criminal conduct (s. 37(2) POCA.). In assessing the proceeds of criminal conduct, the value of a defendant's proceeds of criminal conduct is the aggregate of the values of the payments or other rewards ((s. 37(1)(b) POCA.) In assessing the value of his proceeds of criminal conduct the court makes required assumptions (s. 37(3) POCA) unless those assumptions are shown to be incorrect. (s. 37(4) POCA.) The amount that might be realised and realisable property is "any property held by the defendant" or gifted by the Defendant (s. 39(2) POCA).

46. **Criterion 4.2 –**

a) For a ML investigation, a civil recovery investigation, a detained cash investigation and for a confiscation investigation there are a number of powers under POCA to identify, trace and evaluate property. Section 149 provides that a judge may make a production order requiring the person *i) the application for the order specifies as appearing to be in possession or control of material to produce it to an appropriate person for him to take away, or ii) requiring that person to give an appropriate person access to the material.* Section 156 provides that a judge may make a search and seizure warrant authorising an appropriate person to *i) enter and search the premises specified in the application for the warrant, and to ii) seize and retain any material found there which is likely to be of substantial value (whether or not by itself) to the investigation for the purposes of which the application is made.* Section 161 provides that a judge may make a disclosure order authorising a police or customs officer *to give to any person (that they consider may have relevant information) notice in writing requiring him/her to answer questions, provide information specified in the notice, produce documents, or documents of a description specified in the notice.* Section 167 provides that a judge may make a customer information order that *a financial institution must provide any customer information as it has relating to the person specified in the application.* Section 174 provides that a judge may make an account monitoring order that *the financial institution must, for the period stated in the order, provide account information of the description specified in the order to an appropriate person in the manner, and at or by the time or times, stated in the order.* Section 179 provides that a judge may request assistance *if he/she thinks that there is relevant evidence in a country or territory outside Gibraltar.* This section applies if a person or property is subject to a civil recovery investigation or a detained cash investigation.

b) Section 119(1) of POCA provides that a customs officer or a police officer may seize any cash if he has reasonable grounds for suspecting that it is (i) recoverable property (i.e. proceed of crime as per POCA s.136), or (ii) intended by any person for use in unlawful conduct. The cash seized can be forfeited administratively (section 123 POCA) or by order of the court (section 130 POCA). These proceedings are civil proceedings and thus the standard of proof required is the civil standard namely on the balance of probabilities.

47. A judge may, on an application made to him by an appropriate person, issue a search and seizure warrant (section 156 & 157 POCA) authorising an appropriate person to enter and search the premises specified in the application for the warrant, and to seize and retain any material found there which is likely to be of substantial value to the investigation for the purposes of which the application is made (section 156(4) POCA).

48. Part 3 of the Criminal Procedure and Evidence Act (CPEA) also provides for powers of seizure. A police officer who is lawfully on any premises may seize anything which is on the premises if he has reasonable grounds for believing that it has been obtained in consequence of the commission of an offence; and that it is necessary to seize it in order to prevent it being concealed, lost, damaged, altered or destroyed (section 25 (2) CPEA). The CPEA also contains additional powers of seizure from the premises (section 29 CPEA) and from the person (section 30 CPEA).

49. Anything which has been seized by a police officer or taken away by a police officer may be retained for as long as is necessary in all the circumstances. Such circumstances include but

are not limited to for use as evidence at a trial for an offence; or for forensic examination or for investigation in connection with an offence (section 28 CPEA). When confiscating the benefit of criminal conduct there are powers to make restraint orders (s.59 POCA).

50. Section 32 contains additional powers of retention of seized property under section 29 and 30 of the CPEA.

c) The Courts have the power to take steps to prevent or void actions that prejudice the ability to freeze or seize property that is subject to confiscation. Confiscation and related proceedings are governed by due judicial process. A receiver may be appointed to take possession of realisable property to protect effectively the interest of the court under Section 59(8)(a), 62 and Section 78.

d) Part IV of POCA (Investigations) provides for confiscation investigation (i.e. investigations into (a) whether a person has benefited from his criminal conduct, or (b) the extent or whereabouts of his benefit from his criminal conduct. Some, but not all, special investigative means are available (see EC 31.2).

51. **Criterion 4.3**– There are laws which provide protection for the rights of *bona fide* third parties. POCA S.39(1)(b), 39(4)(b) and 39(5) leave out of the realisable property which is payable in pursuance of obligations which then have priority. When property is being realised by a receiver, s.62(8) gives a reasonable opportunity for any persons holding an interest in the property to make representations to the court. S.140 deals with the exceptions where recoverable property is disposed of but obtained in good faith.

52. **Criterion 4.4** – The Asset Recovery Office within the RGP is responsible for the managing and where necessary, the disposal of frozen, seized or confiscated assets. Part V of POCA headed Civil Recovery of the proceeds etc. of unlawful conduct sets out the powers related to property management for the receiver (s. 82(1) and Schedule 3) and the trustee for civil recovery (s. 91(6) and Schedule 4). These include (a) selling or otherwise disposing of assets comprised in the property which are perishable or which ought to be disposed of before their value diminishes; (b) carrying on, or arranging for another to carry on, the trade or business; (c) incurring capital expenditure in respect of the property. Because FT is unlawful conduct, these powers would be applicable to the instrumentalities and the money/ other property frozen, seized or confiscated under the Terrorism Act 2018.

Weighting and Conclusion

53. Gibraltar meets all the criteria of this Recommendation apart from C.4.2 which is mostly met and for the reason that not all special investigative means are available. **R.4 is rated LC.**

Recommendation 5 - Terrorist financing offence

54. In the 2007 IMF Report, Gibraltar was rated as compliant with S.R.II.

55. **Criterion 5.1** – Gibraltar's FT offences cover the conduct criminalised in Article 2 of the UN Convention for the Suppression of FT (FT Convention). Gibraltar criminalises the provision, receipt, and invitation to provide money or other property with the intent or reasonable suspicion that it may be used for the purposes of terrorism (TA2018, section 35). Under TA2018 it is also an offence to enter into or become concerned in an arrangement which results in money or property being made available to another, where the person knows or suspects that it may be used for the purposes of terrorism (TA2018, section 37). An activity is "for the purposes of terrorism" where (a) there is an act or threat of serious violence, property damage, life endangerment, health or safety risks, or serious electronic interference; (b) the act or threat is designed to coerce, compel or undermine the government or international governmental organisation or to intimidate the

public or a section of the public; and (c) the act or threat is committed with the purpose of advancing a political, religious, racial or ideological cause (TA2018, section 4). It does not matter for the purposes of the terrorist use or threat of action as defined in section 4 where the person or property is situated (section 4(3) b). Included in the definition of terrorism S.4(4) TA 2018: "In this Act a reference to action taken for the purposes of terrorism includes a reference to action taken for the benefit of a proscribed organisation." S. 39A further extends the definition of terrorism and thereby extends that which is defined as for the purposes of terrorism: "39A. For the purposes of sections 35 to 39, the definition of 'terrorism' includes the use or threat of action where the action is one set out in the third column of the table in Schedule 17, and the definition of 'terrorist property' shall be construed accordingly." Any of the Schedule 17 Treaty offence activities are thus for the purposes of terrorism and it is unnecessary, where these apply, to prove any other additional or separate terrorist purpose.

56. The authorities provided references to the legislation covering (whether directly or indirectly) those offences listed in the annex to the Terrorist Financing Convention: (1) (3) and (6) (seizure of aircraft and suppression of unlawful acts against airports and aircraft safety) section 48 of the Civil Aviation Act as read with the CA2011; (3) item 96 in Appendix 1 to the English Law Application Act (internationally protected persons); (4) (hostage-taking) section 24 of the TA 2005 (5) (safeguarding of nuclear material) section 18(10) of the Weapons of Mass Destruction Act (7) and (8) (safety of maritime navigation and fixed platforms) sections 2,3, 5 and Maritime Security Act (*passim*); and (9) (suppression of terrorist bombing), section 135, TA2018 and sections 135-148 of the CA2011. In addition, offences under the nine Conventions and Protocols under the Annex to the TFC, are referred to in section (39A) and Schedule (17) of the Terrorism Act 2018. The funding of any of the conduct described in Schedule 17, irrespective of whether it is otherwise criminalised in the law of Gibraltar, will continue to be a terrorist financing offence (i.e. an offence under one or more of section 35-39 of the Terrorism Act 2018). Consequently, all activities covered by the Conventions and Protocols in the Annex to the FT Convention have been criminalised. The funding of these activities can be pursued as a FT offence where the activity was committed "for the purposes of terrorism" and the necessary elements are met. Where this is not the case, the funding of these activities would be criminalised as aiding and abetting of the criminal act.

57. **Criterion 5.2** – Terrorist financing is criminalised by the TA 2018 (see sec.35-39).

58. The three main FT offences are as follows: Raising funds for terrorism (section 35); Use and possession of money/ other property for terrorism (section 36); Arranging funds for terrorism (sec.37). Section 39 covers the ML of terrorist property where the accused enters into/ becomes concerned in an arrangement of terrorist property (which includes money/ other property likely to be used for the purposes of terrorism) by concealment; by removal from the jurisdiction; by transfer to nominees; or in any other way. The section 35 and section 36 offences require an intention or a reasonable cause to suspect that the property may be used for the purposes of terrorism. The section 37 offence requires knowledge or a reasonable cause to suspect that the property may be used for the purposes of terrorism. The UK Supreme Court in *R. v Lane (Sally) and Another* [2018] UKSC 36 defined the meaning of the words "knows or has reasonable cause to suspect" in the UK's Terrorism Act 2000 as where there existed objectively assessed cause for suspicion. This focused attention on what information the accused had. That requirement was satisfied when, on the information available to the accused, a reasonable person would suspect that the money might be used for terrorism.

59. Terrorism is broadly defined to include terrorist acts and action taken for the benefit of proscribed organisations. Any resources of a proscribed organisation are money/other property for the purposes of terrorism. The offences cover the provision or collection of money or property, directly or indirectly, for use, in full or in part, by an individual terrorist or terrorist group, whether

or not it is linked to a specific terrorist act (The authorities rely on cases from England and Wales: *R v Majdi Shajira* (2015); *R v Hana Khan* (2015); *R v Golamaully and Golamaully* (2016)).

60. The Gibraltar legislation uses the concept of recklessness to criminalise the financing of an individual terrorist or an unproscribed terrorist organisation in the absence of a link to a specific terrorist act or acts. According to paragraph 29 of the FATF Guidance “Criminalising Terrorist Financing (Recommendation 5) , October 2016), “Criminalisation of recklessness as to the use of funds or other assets for terrorist purposes could therefore be considered as consistent with this requirement in some circumstances, although it cannot substitute for criminalising the intentional financing of a terrorist organisation.” As observed above, the case of *R. v Lane (Sally) and Another* is authority for the propositions that the FT offences do not apply a subjective test and “cause for suspicion that funds might be used for terrorist purposes” is objectively assessed.

61. Part 2 of the TA2018 provides for the proscribing of terrorist organisations. Section 10 expressly criminalises providing support for proscribed organisations (irrespective of the purpose of that support).

62. **Criterion 5.2 bis** – Gibraltar criminalises the preparation of terrorist acts, provision of terrorist training (sections 16 and 17 of TA2018), and terrorist financing (sections 35-39 TA2018). As for financing the travel of individuals who travel to another jurisdiction for the purpose of perpetrating, planning, preparing, or participating in terrorist acts or terrorist training, Gibraltar has explicit offences which criminalise these activities: section 22 (Travelling abroad for the purpose of terrorism), section 23 (Funding travelling abroad for the purposes of terrorism) and section 24 (Organising or otherwise facilitating travelling abroad for the purpose of terrorism).

63. **Criterion 5.3** – The FT offences (sections 35-39) apply to money or “other property”. In the TA 2018 Interpretation Section in Part 1 “property” is defined as being “construed widely and includes property of any description including a) assets of every kind, whether corporeal or incorporeal, moveable or immovable, tangible or intangible, and legal documents or instruments in any form including electronic or digital, evidencing title to or an interest in such assets; b) not only such property as has been originally in the possession of or under the control of any person but also any property into or for which the same has been converted or exchanged, and anything acquired by such conversion or exchange whether immediately or otherwise. Terrorist property is also defined at section 5 and includes “money or other property which is likely to be used for the purposes of terrorism (including any resources of a proscribed organisation.)” Neither definition is explicit that money/other property could be terrorist property wherever situated.

64. The definition of property at section 3 quoted above would cover any funds or other assets whether from a legitimate or illegitimate source.

65. **Criterion 5.4** – The FT offences do not require that the funds or other assets were actually used to carry out or attempt a terrorist act or be linked to a specific terrorist act. It is sufficient that there was reasonable cause to suspect that the funds could be used for this purpose - the legislation requires that the person “intends that [the funds] should be used or has reasonable cause to suspect that [they] may be used for the purposes of terrorism” (TA2018, sections 4, 35-37).

66. **Criterion 5.5**. – It is a principle at Common Law that the intent or reasonable cause to suspect required to prove an offence may be inferred from objective factual circumstances (see 3.8 above.)

67. **Criterion 5.6** – FT is punishable by proportionate and dissuasive criminal sanctions with a maximum penalty of 14 years imprisonment or a fine or both for natural persons (s.54 Terrorism Act 2018).

68. **Criterion 5.7** – Criminal liability and sanctions apply to legal persons, without prejudice to the criminal liability of natural persons (sanctions can apply to either or both). Offences committed by legal persons are punishable by a fine. Criminal liability and sanctions apply to legal persons by virtue of section 2 of the Interpretation and General Clauses Act 1962 which includes within the ambit of 'person' any corporation either aggregate or sole, and any club, society or other body . . ." Corporate criminal liability does not prejudice the criminal liability of a natural person. Additionally, section 3(1) of the TA 2018 ('Interpretation') defines a Gibraltar resident to include a body incorporated in Gibraltar.

69. **Criterion 5.8** – Gibraltar's FT offences are broad in nature. Attempts, inchoate offences and conspiracy in relation to the FT offences are not explicitly covered in the Terrorism Act 2018 but are included in general provisions of the criminal law of Gibraltar. These provisions cover the a) attempts to commit an offence (s. 22 Crimes Act 2011); b) encouraging or assisting the commission of an offence (ss. 36 and 37 CA 2011); c-d) a conspiracy to commit an offence (s. 27 CA 2011); a conspiracy to commit an offence outside Gibraltar (s. 28 CA 2011); aiding and abetting counselling, procuring or suborning the commission of an offence (s. 47 CA 2011).

70. **Criterion 5.9** – The FT offences are indictable offences and therefore ML predicate offences (POCA S. 182(I)). Section 39 of the TA 2018 also creates a specific ML offence: if a person enters into or becomes concerned in an arrangement of terrorist property by concealment, by removal from the jurisdiction, by transfer to nominees or in any other way.

71. **Criterion 5.10** – Gibraltar's FT offences apply regardless of whether the defendant was in the same country or a different country from the one in which the terrorist or terrorist organisation is located, or where the terrorist act occurred or will occur (s. 4(3) TA2018).

Weighting and Conclusion

72. All criteria are met. **R.5 is rated C.**

Recommendation 6 - Targeted financial sanctions related to terrorism and terrorist financing

73. In the 2007 IMF report, Gibraltar was rated largely compliant for former SR.III. The report noted a disconnection in the financial community concerning their affirmative obligations under the UNSCR 1267 and EU regulations. In 2019, Gibraltar adopted the Sanctions Act addressing most of the issues required under R.6.

74. **Criterion 6.1** – In relation to designations pursuant to UNSCR 1267/1989 and 1988: Gibraltar is obliged to take action against persons and entities listed by the UNSC 1267 and 1988 Committees. It meets this obligation by directly and automatically incorporating the designations made by those Committees into its domestic legislation via the Sanctions Act 2019 (S.7 and 8).

a) The Chief Minister is the competent authority responsible for proposing designations as per Section 14 of the 2019 Sanctions Act. In effect, the proposal for designation has to be made via the United Kingdom, to the UNSC (Gibraltar cannot propose a designation directly to the UN because of its constitutional and international status). In this regard, section 14(5) of the Sanctions Act requires the Chief Minister to coordinate the proposal of UN designations with the Foreign and Commonwealth Office. The execution of such a designation proposal would be made via a Memorandum of Understanding that has been concluded between HMGoG and the UK Foreign & Commonwealth Office and which entered into force on 4 April 2019.

b) Following the approval of the Sanctions Act, the authorities introduced standard forms for listing of groups, entities and individuals on the Isil (Da'esh) and Al-qaida sanctions lists which

replicate the criteria set out in the UNSCRs. Gibraltar authorities also advised that the primary mechanism for identifying targets would be intelligence gathering and sharing among Gibraltar, Gibraltar-UK and Gibraltar-international agencies, which would be reviewed against the criteria set out in the UNSCRs. Furthermore, section 14(2) of the Sanctions Act provides mechanisms upon which the Chief Minister shall, for the purpose of subsection 1 (i.e. identifying targets and requesting listing by the United Nations Security Council), take into consideration such information and intelligence as he may be made aware of by:

(i) a police officer, an officer of HM Customs, the Gibraltar Co-ordinating Centre for Criminal Intelligence and Drugs (GCID); or the Gibraltar Financial Intelligence Unit (GFIU);

(ii) the Gibraltar Contingency Council,

(iii) such other person or body as he considers appropriate in the circumstances;

c) The evidentiary standard of proof applied to a designation proposal is a 'reasonable belief' of a potential designee's association with terrorism – Section 14(3)(a) of the Sanctions Act. The decision is not conditional on the existence of a criminal proceeding (Section 14(3)(b)).

d) As noted, Gibraltar is not a member of the UN. However, in light of section 14(5) of the Act and of the agreement/MOU with the UK in regard to designation proposals, UN standard forms and procedures have been adapted as templates, with necessary modifications.

e) Subsection 14(4) of the 2019 Sanctions Act provides that the Chief Minister shall provide all the relevant data sufficient for identification of the potential designee, reasons why the proposed designation meets the Gibraltar legal test and unclassified information about the Gibraltar-held assets of the proposed designated person, along with any information about the potential designee's connections with Gibraltar.

75. **Criterion 6.2** – In relation to designations pursuant to UNSCR 1373: Gibraltar implements designations pursuant to UNSCR 1373 through both Gibraltar and European mechanisms. The Gibraltar mechanism is found in the Terrorist Asset Freezing Regulations (TAFR) and section 15(1) of the Sanctions Act 2019; the European mechanism is found in CP 2001/931/CFSP and Council Regulation 2580/2001. Moreover, section 7(1) of the Sanctions Act 2019 also serves to incorporate European Union sanctions lists directly into Gibraltar's domestic legal order.

a) The Chief Minister and Minister for Financial Services are responsible for designations under TAF Regulations (s 4(1)) European Union designations pursuant to UNSCR 1373 apply automatically by virtue of section 7(1) of the Sanctions Act 2019. Proposals for designations to the European Union would be made by the Chief Minister pursuant to the mechanism in section 7A of the Sanctions Act 2019. The EU is responsible for deciding on the designation of persons or entities (Regulation 2580/2001 and Common Position 2001/931/CFSP) and relies on a prior decision of a competent authority.

b) The same process to the one described under c.6.1(b) would be applied to identifying targets for designations based on the UNSCR 1373 criteria.

c) Section 16B of the Sanctions Act 2019, read in conjunction with Section 15 (specifically section 15(1) a)) provides for the Chief Minister to determine a designation request from abroad with seven days of receiving the request and to inform the requesting jurisdiction of the determination. The Chief Minister has the power to solicit information and intelligence from specified persons and bodies (and others) he considers appropriate (16A of the Sanctions Act 2019). The existence of criminal proceedings is expressly excluded as a condition for a designation (section 16B(4)(b) of the Sanctions Act 2019). The evidentiary threshold that a requesting foreign jurisdiction must meet for the Chief Minister to make a designation is 'reasonable belief' (section 16B(4)(a)).

d) In deciding whether to make a designation, the Chief Minister would use the evidentiary standard of proof of 'reasonable grounds' pursuant to section 15(1) of the Sanctions Act 2019. The evidentiary standard of proof for a designation by the Minister for financial services under the TAF Regs is 'reasonable belief' (regulation 4(1) of TAF Reg.).

e) When requesting another country to give effect to freezing mechanisms, Gibraltar must provide identifying and supporting information. This is provided for in section 16C of the Sanctions Act 2019.

76. Criterion 6.3 –

a) The Chief Minister has the power under section 16A of the Sanctions Act 2019 to solicit information for the specific purpose of assessing whether there are reasonable grounds for a designation. In addition, R.31 outlines the provisions for collection or solicitation of information to identify persons and entities that may meet the criteria for designation.

b) It can be deduced from the TAF Reg. and 2019 Sanctions Act (both do not require a person to be notified, consulted or present as part of the designation process)⁹⁴ that the Minister has implied powers to operate *ex parte*. Designations by the UN under the sanctions regimes are made on an *ex parte* basis, and EU designations are required to be made *ex parte*.

77. Criterion 6.4 – Designations pursuant to the UN sanctions regimes are immediately effective in Gibraltar, as are designations implemented through EC regulations (sections 6(2) and 7(1) of the Sanctions Act 2019). The legislation specifically states that *international sanctions (imposed by UNSC, EU, those imposed under the UK Terrorism Freezing Act and any restrictive measures notified by the Government of Gibraltar) have effect in Gibraltar on the date and, where applicable, the time in which they are intended to come into operation by the international body that has imposed them.*

78. Criterion 6.5 –

a) All natural and legal persons in Gibraltar, and persons and bodies constituted under Gibraltar law, wherever they are located, are required to freeze the funds or economic resources of a designated person, without delay and without prior notice (section 8(3) c) of the Sanctions Act 2019; TAF Regs 16(1), EC Regulations 881/2002 art.2(1), 1286/2009 art.1(2), 753/2011 art.3, 754/2011 art.1 and 2580/2001 art.2(1a)). A person who fails to comply with a requirement to freeze commits an offence See also analysis in 6.3-6.4.

b) Freezing actions pursuant to Part 5 of Terrorism Act 2018 and the TAFR, and at the EU level (under the 1267/1989 and 1988 regime), apply to funds or economic resources owned, held or controlled, directly or indirectly, by a designated person/entity (TAF Regs regulation 4(1)a(ii); EC regulation 881/2002, art.2; EC regulation 753/2011, art.3). This extends to interest, dividends and other income on or value accruing from or generated by assets (TAFR, regulation 13(1)(d) and see definition of funds in the EC regulations, art.1). The Minister may make a final and/or an interim designation of a person if he/she is owned or controlled directly or indirectly by a person involved in the terrorist activity, or is acting on behalf of or at the direction of that person and restrictions should then be applied in relation to the person – TAFR (regulation 4(1) and 8(1)(a)(iii)). Equally, the requirement to freeze funds or assets 'controlled' directly or indirectly by a designated entity is also a part of the EC regulation 881/2002, art.2.

⁹⁴ This kind of power in common law is the power of Ministers that would be constrained by express statutory language or human rights legislation only (e.g. as regards an abusive exercise of the *ex-parte* power).

79. For UNSCR 1373, the freezing obligation in EU regulation 2580/2001 (Article 1(a) and Article 2(1)(a)) applies to assets belonging to, owned or held by the designated individual or entity, and does not expressly apply to funds or assets controlled by, or indirectly owned by, or derived from assets owned by, or owned by a person acting at the direction of a designated person or entity. However, this gap is largely addressed as the European Council is empowered to designate any legal person or entity controlled by, or acting on behalf of, a designated individual or entity (EU regulation 2580/2001, Article 2(3) (iii) and (iv)) and by the TAFR (regulation 4(1)a (ii) and (iii)).

80. EU regulations do not expressly require the freezing of jointly owned assets. This has not been covered by Gibraltar legislation either, although authorities advised that, in practice, jointly held assets may be frozen particularly if there is a risk that funds or assets will become available to a designed person or entity.

c) Part III of the TAF Regs ('Prohibitions in Relation to Designated Persons'), regulations 17-20, prohibits a person⁹⁵ from making funds, financial services or economic resources available to a designated person or for the benefit of a designated person (see also section 37(a) TA 2018 which criminalises *arranging funds for terrorism*).

81. The prohibition for the part "acting on behalf of, or at the direction of, designated persons or entities" is directly covered in Part I (regulations 4(1)(a)(iii) and 8(1) of TAFR).

d) Authorities indicated regulation 5 of the TAF Regs ('the Minister must take steps to make public the designation generally...') as a basis for communicating the designations. The Sanctions Act also contains further enabling provisions under section 24(4). The GFIU maintains a dedicated webpage with regard to TFS (<http://www.gfiu.gov.gi/sanctions>). This website directs the reader to the relevant UN lists. A financial sections guideline has been published by the GFIU http://www.gfiu.gov.gi/uploads/UcjV5_Financial_Sanctions_Guidance_Notes_v1.0.pdf. A consolidated list of all target freezes is published on <https://www.gov.uk/government/publications/financial-sanctions-consolidated-list-of-targets/consolidated-list-of-targets>. Gibraltar-specific designations is also listed on the GFIU's website - sanctions webpage. The authorities advised that the preceding website is updated within one business day. Regulation 5 of the TAFR as amended (on 4 April 2019) imposes an obligation to communicate designations to the financial sector and the DNFBPs *immediately*.

e) Reporting obligations of relevant institutions are covered under TAFR (regulation 24) and Schedule 4 to the Sanctions Act 2019. The combined effect of sub-regulations 24(1) and (4), are that a *relevant institution* must state the nature and the amount or quantity of any funds or economic resources held by it for the customer (i.e. designated person) at the time when it first had the knowledge or suspicion and does not refer to 'frozen assets or actions taken' in compliance with the prohibition requirements. Read together with sub-regulation 24(4), which requires that '*the relevant institution must also state the nature and amount or quantity of any funds or economic resources held by it for the customer at the time when it first had the knowledge or suspicion.*', and sub-regulation 24(5), which criminalises failure to report, it can be concluded that the reporting requirement is covered, although indirectly.

82. In addition, the definition of "relevant institution" under the TAF Regs (regulation 15. (1)) makes specific reference to FIs and DNFBPs. Attempted transactions are covered under section 8(3)(c) of the Sanctions Act 2019.

⁹⁵ 'Person' is defined in the Interpretation and General Clauses Act as including 'any corporation either aggregate or sole, and any club, society or other body, or any one or more persons of any age, and either of the male or female sex', and therefore covers entities. The Interpretation and General Clauses Act applies to all Acts unless the context otherwise requires.

f) There are no direct provisions covering the requirement of this criterion. However, regulation 32 (2) of the TAFR allows 'any person affected by a decision' to apply to the Supreme Court to review decisions taken by the Minister (ergo this includes third parties). Also, Section 58(1) of the Terrorism Act grants third parties a right to be heard in forfeiture proceedings. Importantly, the rights of bona fide third parties are protected under the EU sanctions regime (Regulations 881/2002 art.6; 753/2011 art.7) directly applicable in Gibraltar. Third parties may have protection under common law against any external challenges provided they had implemented the asset freeze as per their legal requirements.

83. **Criterion 6.6 –**

a) The Sanctions Act 2019 at sections 12 and 13 provides for a mechanism in Gibraltar to de-list persons and entities which do not or no longer meet the criteria for designation. Whilst the legislation does not refer directly to unfreezing of funds or other assets of designated persons or entities, the authorities advised that once a designation is lifted, assets are automatically unfrozen (i.e. the nature of 'freezing' in the UK and Gibraltar legislative schemes is effectively one of a designation which prohibits the target and anyone else from dealing with the assets – except under license, etc.).

84. HMGoG and the UK Foreign Office signed a MoU for a mechanism whereby Gibraltar can make proposals for de-listing to the UN via the UK as Gibraltar does not have its own representation in the UN.

85. In addition, other relevant procedures are set out in the Financial Sanctions Guidance: http://www.gfiu.gov.gi/uploads/UcjV5_Financial_Sanctions_Guidance_Notes_v1.0.pdf. The guidance explains how to challenge the UN ISIL (Daesh) AQ regime through the UN Office of the Ombudsperson, for the other UN listings through the UN focal point for delisting. Alternatively, a UK resident or citizen can petition the UK to submit a delisting request to the UN. This can be done through the FCO Sanctions Section. For EU listings a designated person should write in the first instance to the EU a determined specified email address.

86. For UK listings, there are avenues of appeal and judicial review within the specific legislation under which the designation is made. There are also indications of the email address for the cases in which a person has been de-listed, but their name still appears on the consolidated list, or its assets have been frozen mistakenly.

87. The delisting process described above is explained in the above-mentioned Financial Sanctions Guidance at the website mentioned.

b) In line with TAFR, designations last one year but can be renewed (regulation 6(1)). The Minister is required to give a written notice of that fact to the designated person and also bring the expiry or revocation of a designation to the attention of persons that were informed of the designation (regulations 6(5) and 7(2)(b)). The Minister may vary or revoke an interim designation at any time (Reg. 7). Where an interim designation is varied or revoked the Minister must (a) give written notice of the variation or revocation to the designated person; and (b) take reasonable steps to bring the variation or revocation to the attention of the persons informed of the designation. According to the authorities, 1373 designations de-listings are immediately effective but beside the power of the minister to vary or revoke a final designation at any time no further procedures are in place.

88. EU de-listing procedures (by Working Party on implementation of Common Position 2001/931/CFSP on the application specific measures to combat terrorism) is immediately effective and automatically recognised in Gibraltar.

c) Regulations 31 and 32 of the TAF Reg. permit applications to be made to the Supreme Court of Gibraltar to review designations. Designations made under the EU's UNSCR 1373 sanctions regime may be challenged through the Court of Justice of the European Union as per the Treaty of Functioning of the EU – Article 263(4). Procedures discussed under criterion 6.6(a) are applicable in this case.

d) Persons designated pursuant to UNSCRs 1267 and 1988 would be informed of the listing, its reasons and legal consequences, as well as their rights of due process and the availability of de-listing procedures (e.g. UN Office of the Ombudsperson or the UN Focal Point mechanism) on the basis of section 28(3) of the Sanctions Act 2019 *[...] the Chief Minister must without delay take such steps as are reasonably practicable to inform the designated person of the designation, variation or revocation [...]*. At the EU level there are procedures that provide for de-listing names, unfreezing funds and reviews of designation decisions by the Council of the EU (EC Reg. 881/2002, art 7A).

e) Same analysis applies for this sub-criterion as for 6.6(d).

f) Gibraltar Financial Services Commission website has a dedicated web-site for terrorist name designations <https://www.fsc.gi/financialcrime/sanctionsandterrorism>. The Gibraltar Financial Intelligence Unit at <http://www.gfiu.gov.gi/sanctions> provides information and general guidance, including links to delisting processes and consolidated lists. The guidance includes general guidance and also a service to ensure that persons or entities with the same or similar names to sanctioned persons or entities are not mistakenly sanctioned ('false positives'). This is necessary where persons or entities do not receive a satisfactory answer from the relevant institution which froze their assets

g) Regulations 6(5) and 7(2)(b) of the TAFR require the Minister to take reasonable steps to bring the expiry or revocation (or, where applicable, variation) to the attention of persons informed of the designation. However these provisions do not provide mechanisms for communicating de-listings and unfreezing and it is therefore necessary to look to the GFIU's Financial Sanctions Guidance in respect of the de-listing or unfreezing action (e.g. paragraph 2.1, which suggest any person who has been de-listed but his/her name still appears on the consolidated list, to contact the Gibraltar competent authority via email (exact address is provided therein) with evidence of de-listing, such as the relevant EU regulation.

89. **Criterion 6.7** – The licensing system in section 10 of the Sanctions Act 2019 is designed to permit access to funds for exceptional reasons in accordance with UNSCR 1452, where applicable, UNSCR 1373. The licensing regime in Articles 4, 5(c), 7, and 13 of the Terrorism (United Nations Measures) (Overseas Territories) Order 2001 is also relevant for purposes of this criterion compliance. At the EU level there are procedures in place to authorise access to frozen funds or other assets which have been determined, amongst others, to be necessary for basic expenses, for the payment of certain types of expenses, or for extraordinary expenses pursuant to UNSCR 1452 (EC Regulations 753/2011, art. 5; 881/2002, art. 2a). Detailed guidance on these measures' application is provided at <http://www.gfiu.gov.gi/sanctions>. This link also provides a link to the UK consolidated list of sanctions (<https://www.gov.uk/government/publications/financial-sanctions-consolidated-list-of-targets/consolidated-list-of-targets>), which comprises UN, EU and UK sanctions and which is directly relevant to Gibraltar by virtue of the applicability of these sanctions pursuant to section 6(2) of the Sanctions Act 2019.

Weighting and Conclusion

90. The legislation in Gibraltar provides sound basis for implementation of targeted financial sanctions related to terrorism and terrorist financing. Still, there are some minor deficiencies, i.e.

the requirement to freeze assets that are jointly owned is not expressly stated in the legislation.
R.6 is rated LC.

Recommendation 7 – Targeted financial sanctions related to proliferation

91. Requirements under Recommendation 7 were not assessed in 2007 IMF report.

92. **Criterion 7.1**– UN financial sanctions are implemented by virtue of EU Regulations. EU Regulations have direct effect in Gibraltar. UNSCR 1718 on DPRK is transposed into the EU legal order through EC Regulation 2017/509 (as amended) and Council Decision 2016/849/CFSP. For Iran, UNSCR 2231 is implemented at the EU level through EC Regulation 267/2012 (as amended). As regards DPRK, Gibraltar has taken the further measure of implementing Council Decision 2016/849/CFSP (via EU Regulation 2017/330) in its Democratic People’s Republic of Korea Sanctions Order 2018⁹⁶. As regards Iran, the UK’s Iran (European Union Financial Sanctions) Regulations 2016 apply to British Overseas Citizens deriving citizenship through a connection with Gibraltar (para. 1(3)(b)) and Gibraltar can receive information from the UK Treasury to facilitate compliance with EU Regulation 267/2012 (para. 5(2)(b)(v)) (including facilitating action with a view to proceedings for an offence in the UK or Gibraltar (paras. 5(3)(i) and (ii)). Additionally, section 7(1) of the Sanctions Act 2019 applies international sanctions automatically and sections 15(1) and (2)(iii) of the Sanctions Act 2019 provide for the Chief Minister to make regulations expressly for the prevention of the proliferation of weapons of mass destruction. The Sanctions Act, therefore, enables immediate transposition of the UN financial sanctions and prevents possible scenario of delays in transposition of UN designations into EU law.

93. These mechanisms include direct provisions for implementation of targeted financial sanctions to comply with UNSCRs related to prevention, suppression and disruption of financing of proliferation of weapons of mass destruction without delay.

94. **Criterion 7.2** – The Chief Minister and the Minister responsible for finance are the competent authorities for implementation of TFS in Gibraltar.

a) EU Regulations require all natural and legal persons within the EU to freeze the funds or other assets of persons or entities designated under the EU’s anti-proliferation regimes. These regulations are supplemented by: (a) a Gibraltar domestic instrument which make it an offence, in respect of the DPRK, for all natural and legal persons not to freeze assets pursuant to the EU’s anti-proliferation measures (the Democratic People’s Republic of Korea Sanctions Order 2018 – Sections 4 – 8)); and (b) the UK’s Iran (European Union Financial Sanctions) Regulations 2016⁹⁷.

b) The EU regulations prohibit dealing with funds or economic resources owned, held or controlled by a designated person, and prohibit making funds, financial services and economic resources available to a designated person or for their benefit. The same prohibitions, expressly including restrictions on financial services and markets, are given effect by regulations in the Democratic People’s Republic of Korea Sanctions Order 2018. The freezing obligation under the EU framework extends to all types of funds (EC Regulation 329/2007, art.1(4) & 6; EC Regulation 267/2012, art.1(l) & 23(1-2)). This requirement extends to funds or assets that are owned, held or controlled by a designated person/entity (e.g. EC Regulation 329/2007, art.6(1). The UK’s OFSI

⁹⁶ Under the relevant EU Regulations, the prohibition to prevent funds, financial services and economic resources being made available applies to British persons and any other legal person, or body incorporated or constituted under Gibraltar law. This applies to anyone residing or located in the UK and UK nationals living overseas in respect of the DPRK (Section 28 of the Democratic People’s Republic of Korea Sanctions Order 2018 - <https://www.gibraltarlaws.gov.gi/articles/2018s002.pdf>).

⁹⁷ Part 1 Section 1 (c) of the regulation states that it is applicable, inter alia, to a British Overseas Territories citizen who acquired their citizenship from a connection with Gibraltar.

Guidance accessible to Gibraltar REs via Gibraltar FIU webpage (pls see EC 6.5 d)) states that where there is an evidenced causal link, the requirement to freeze the funds or assets 'controlled' by a designated person also extends to and the funds or assets belonging to people who are acting on behalf of or at the direction of designated persons/entities accessible through Gibraltar FIU webpage [http://www.gfiu.gov.gi/uploads/UcjV5 Financial Sanctions Guidance Notes v1.0.pdf](http://www.gfiu.gov.gi/uploads/UcjV5_Financial_Sanctions_Guidance_Notes_v1.0.pdf). The EU Regulations do not expressly require the freezing of jointly owned assets. However, GFIU guidance provides methods how to freeze jointly owned assets (detailed in paragraphs 1.1.7, 1.1.11, 2.15, 2.16, 3.1.14 and 3.1.15 of the GFIU's Financial Sanctions Guidance) and this could be used as point of reference in Gibraltar.

c) Under the relevant EU Regulations, the prohibition to prevent funds, financial services and economic resources being made available applies to British persons and any other legal person, or body incorporated or constituted under Gibraltar law. This applies to anyone residing or located in the UK and UK nationals living overseas in respect of the DPRK (para. 28 of the Democratic People's Republic of Korea Sanctions Order 2018 – see also EC 7.1).

d) The GFIU maintains a dedicated webpage with regard to TFS (<http://www.gfiu.gov.gi/sanctions>). This website directs the reader to the relevant UN lists. As already noted under previous essential criteria under R.6, the webpage includes the links to the financial sections guideline published by the GFIU and the OFSI's consolidated list of all target freezes <https://www.gov.uk/government/publications/financial-sanctions-consolidated-list-of-targets/consolidated-list-of-targets>. The preceding website is updated within one business day. The authorities advised that FIs and DNFBPs within the regulatory remit of the GFSC are also informed immediately via email of any sanctions designations related to proliferation financing. Similarly, the GFSC's website is updated with any new designations or changes to existing designations. The authorities consider this as a mechanism of communicating designations and changes with regard to them. This mechanism has been detailed in the GFSC's Financial Crime Team Procedures Manual (page 29 of the manual).

e) Council Regulations (EU) 2017/1509 and (EU) 267/2012 are directly applicable in Gibraltar. Article 50 of the (EU) 2017/1509 and Article 40 of the (EU) 267/2012 impose that FIs and DNFBPs must immediately provide to the competent authorities all information to facilitate compliance with the EU regulations, including information about the frozen accounts and amounts. In addition, FIs and DNFBPs are required to report to the Minister responsible for finance if they know or have reasonable cause to suspect that a person is a designated person or has done something in contravention of the TFS regime pursuant to para. 31 (Schedule (Information Provisions)) of the Democratic People's Republic of Korea Sanctions Order 2018. These provisions are sufficiently broad to cover reporting on attempted transactions.

f) The rights of bona fide third parties are protected by the relevant EU regulations which are directly applicable in Gibraltar (Council Regulation (EU) 2017/1509, art.50; Council Regulation (EU) No 267/2012, art.42).

95. **Criterion 7.3** – FIs and DNFBPs are required to report to the Minister responsible for finance if they know or have reasonable cause to suspect that their customer is a designated person or that a breach has occurred, or if they have frozen funds under the relevant regulations. The Minister also has powers to request information from relevant institutions or designated persons in relation to sanctions evasion (Democratic People's Republic of Korea Sanctions Order 2018 – Schedule (Information provisions) – paras. 1(1) to (5); Section 40 of 2018 Terrorism Act and regulation 24 of TAFR). It is a criminal offence to breach the freezing and prohibition of the provision of funds and the information gathering and information disclosure provisions. The

criminal penalties range between 3 months and 2 years in prison (Democratic People's Republic of Korea Sanctions Order 2018, paras. 24, 25 and 27 and the Schedule).

96. The Minister may request any person in or resident in Gibraltar to provide information as he reasonably requires for the purpose of monitoring compliance with or detecting evasion of the Democratic People's Republic of Korea Sanctions Order 2018 (para. 2(5)(b) of the Schedule). Although the authorities advised that the GFSC supervises FIs and DNFBPs on PF matters in the exact same way as it does for ML and TF (i.e. ensuring compliance with PF sanctions and that these are integrated into the firms' policies and procedures – analysis of IO11 confirms that this is the case – please see paragraphs 301 and 313 therein) no provision covers this issue.

97. **Criterion 7.4 –**

a) HMGOG and the UK Foreign Office concluded an MoU for a mechanism whereby Gibraltar can enforce its power to make proposals for designation to the UN or EU Council (the latter in order to meet the requirements of Regulation 2580/2001 and Common Position 2001/931/CFSP) via the UK as Gibraltar does not have its own representation in either body.

98. In this regard, the sanctions page in the Gibraltar FIU's website directs to the relevant procedures, i.e. GFIU Financial Sanctions Guidelines, similarly as is the case under 6.6 a)

99. Designated persons who have been subject to sanctions are able to challenge their listing and request their delisting. The financial sanctions will remain in place while the challenge or request is being considered. A request for delisting can be made through the mechanism in section 12, 13 or 13A (as appropriate) of the Sanctions Act 2019 and could also be sent to the UN focal point for delisting for which the web site is indicated. Court reviews of decisions are provided for in Part 4 of the Sanctions Act 2019.

100. Alternatively, a UK resident or citizen can petition the UK to submit a delisting request to the UN.

101. The EU Council communicates its designation decisions and grounds for a listing to designated persons, who have the right to request a review of the EU decision independently of whether a request is made at UN level (Treaty on the Functioning of the European Union (TFEU), in the fourth paragraph of art. 263 & 275).

b) There are publicly known procedures (available from the sanctions section of the GFIU website) for obtaining assistance to be able to check whether persons or entities having the same or similar names as designated persons or entities are mistakenly subjected to an asset freeze ('false positives'). These procedures are available on the GFIU web-page (<http://www.gfiu.gov.gi/sanctions>) and provide for the affected person to contact the GFIU or the RFB directly (see paragraphs 2.2 and 8.4 of the GFIU Financial Sanctions Guidance).

c) The competent authority operates a licensing system to allow designated persons or entities access to funds as required by EU Regulations 267/2012 and 2017/1509 (Part 4 of the Democratic People's Republic of Korea Sanctions Order 2018). UN and EU de-listings are reflected in the consolidated list of financial sanctions targets within one business day. The consolidated list can be accessed through the GFIU website which directs the user to the GFIU's Financial Sanctions Guidance and the OFSI's consolidated lists of all asset-freeze targets (<https://www.gov.uk/government/publications/financial-sanctions-consolidated-list-of-targets/consolidated-list-of-targets>).

102. **Criterion 7.5 –**

a) Gibraltar applies European regulations for this purpose which permit payment to the frozen accounts of interest or other sums due on those accounts or payments due under contracts,

agreements or obligations that arose prior to the date on which those accounts became subject to the provisions of this resolution provided that these amounts are also subject to freezing measures (Art. 34 Regulation 2017/1509 and Art. 29 Regulation 267/2012). Art. 25 Regulation 267/2012 authorise the payment of sums due under a contract entered into prior to the designation of such person or entity, provided that this payment does not contribute to any activity prohibited by the regulation, and after prior notice is given to the UN Sanctions Committee.

With regard to the freezing measures pursuant to UNSCR 2231, special provisions set out in Regulation 267/2012 (Art. 24 and 25) authorise the payment of sums, due under a contract which arose prior to the designation of such person or entity, provided that this payment does not contribute to an activity prohibited by the regulation (and de facto the UNSCR), and after prior notice is given to the UN Sanctions Committee.

Weighting and Conclusion

103. As noted under R.6, a mechanism to list and de-list persons and entities with regard to targeted financial sanctions related to proliferation has become operational in light of the MoU signed with the UK. No provision specifically requires supervisors to monitor and ensure compliance by FIs and DNFBPs with proliferation financing sanctions although in practice such supervisions were carried out. **R.7 is rated LC.**

Recommendation 8 – Non-profit organisations

104. In the 2007 IMF assessment report, Gibraltar was rated LC with former SR. VIII. The main deficiencies were the Board members were unaware of the provisions of the FATF's guidance on the possible abuse of NPOs for FT purposes; and the blanket exemption from registration to religious charities was inconsistent to the sector's FT risk.

105. ***Criterion 8.1*** –

a) A NPO FT risk assessment was performed in April 2017, including the identification of the subset of organisations that fall within the FATF definition and those NPOs that are more likely to be at risk of FT abuse. The National Coordinator (NCO) developed a questionnaire seeking to better understand the size, the nature of the NPO activities, the geographical location of their work and source of funding. The questionnaire was sent to all charities and friendly associations. Information from the banking sector, the Board of Charities and the Registrar of Friendly Societies (RFS) was also considered. The risk assessment concluded that the NPO sector of Gibraltar is small, with few exceptions referring to community development and education charities. The FT risk of the sector was assessed to be low and no evidence of FT abuse was found. The assessment included a recommendation to the Board of Charity Commissioners to continue monitoring the risk indicators for educational grants to non-Gibraltar based beneficiaries and charities with poor systems of control.

b) The 2017 NPO assessment assigned a low FT risk to the sector. In view of the absence of evidence of FT abuse, the 2018 NRA assessed the threat to collect and transfer funds through NPOs for FT purposes to be medium to low. The NRA also highlights that criminals may abuse NPOs to fund localised terrorist activities or may seek to use NPOs to facilitate cross-border financing by sending money to areas where the NPOs are operating close to terrorist areas of activity.

In August 2017, the authorities communicated a newsletter to all charities and friendly societies providing information on a number of methodologies for abuse by terror actors: diversion of funds; affiliation with a terrorist entity; abuse of programming and support for recruitment. However, as outlined in the newsletter these typologies derived from the FATF paper titled "Risk of terrorist abuse in NPOs" rather than Gibraltar's own analysis and thus might not

necessarily fully reflect Gibraltar's NPO sector vulnerability in light of the NRA findings. The authorities have confirmed that the risk indicators from that paper were assessed against the presence (or otherwise) in the Gibraltar NPO Sector.

c) In the aftermath of the 2017 risk assessment, the NCO conducted a review of the current provisions of the Charities Act (CharA) and Friendly Societies Act and determined that the existing measures are adequate based on the NPO risk assessment, and current registration and oversight requirements. During this process, input from both the Board of Charities Commissioners (BCC) and the RFS was also taken into account.

The authorities have also identified an area of improvement which refers to the establishment of a formal communication gateway between the Board of Charity Commissioners, financial regulators and the GFIU in order to facilitate the exchange of concerns and information. Another action, which was also included in the 2017 NPO Risk Assessment Actions to expand the investigatory powers provided in S8(1) and S9(1) of the CharA.

d) Since 2017, the sector has been reviewed twice as subject of a sector-specific assessment and the NRA. In addition, bearing in mind its small size, the sector's vulnerabilities are kept under review by the Board of Charity Commissioners, the RFS and GFIU.

106. Criterion 8.2 –

a) Although there is no specific policy document on the promotion of transparency, integrity and public confidence in the administration and management of NPOs, legal requirements can be found in the CharA (Section 4(3, 4)) and the Friendly Societies Act (and Rules).

b) With regard to the NPO sector the NCO prepared and distributed a survey on the FT vulnerabilities of the sector which was used in preparation of the 2018 NRA. In addition, a Newsletter on FT Risks was communicated to all NPOs in August 2017, while in May 2018 presentations were held to the NPO Sector focusing on FT Risks identified in the FT Risk Assessment under the GFIU's Project Nexus outreach programme.

No outreach or educational programmes to donors has been conducted.

c) The authorities provided information on the 2018 NPO Presentation of June 2018 in relation to the FT risk of the sector. This included information for NPOs for how they could protect themselves against FT Risk including specific measures to be taken. The Presentation was prepared and presented by the NCO. No NPOs were involved in this initiative to develop and refine best practices to address terrorist financing risk and vulnerabilities and thus protect them from terrorist financing abuse;

d) Through the 2018 presentations on NPOs FT risk, the authorities have encouraged all charities and friendly societies (FS) to conduct transactions via regulated financial channels. In addition, the authorities have confirmed that charities in Gibraltar conduct all their donation work via regulated channels (mainly banking services). The authorities also informed that FS receive mutual help only in kind or through banking services.

107. Criterion 8.3 – There are two types of NPOs: charities and friendly societies.

Charities

108. They are supervised and monitored by the Board of Charity Commissioners for Gibraltar. The Board of Charities is governed by the CharA. The Board holds meetings periodically around four times a year on average. Charities in Gibraltar are registered with the Board of Charity Commissioners and the register is publicly available for inspection. A number of registration requirements are set in the law and policies. In the least, a charity is expected to have a connection with Gibraltar and that there would need to be locally resident Trustees. The application for registration among other documents must be supported by the objectives of the proposed

Charity/Trust and the obligation to inform the Board of Charities on any changes. Applications for registration are generally accompanied by a cover letter stating from where the proposed Charity will source its funds, who the beneficiaries will be and how it intends to raise funds going forward.

109. A unique registration number is assigned to every charity registered in the Register of Charities. In respect of accounts, an annual Income and Expenditure account, a Balance Sheet and an annual brief report on the charity's activities shall be submitted to the Register, no later than six months following the end of a financial year. The obligation to maintain accounts is contained in section 31 of the CharA. Accounts must be signed off by no less than two Trustees. Audited accounts are required in the case of charities where the income and/or distributions exceed fifty thousand pounds per annum. All annual accounts are scrutinised by two Commissioners and their observations are subsequently reported to the Board.

Friendly Societies

110. The purpose of friendly societies is set out in section 3 of the Friendly Societies Act. Friendly societies are registered with the Registrar of Friendly Societies. A friendly society consists of a minimum of seven persons. No society which contracts with any person for the assurance of an annuity exceeding GBP 104 per annum or of a gross sum exceeding GBP 500 may be registered under the Act. Every registered society must have a registered office to which all communications and notices are addressed.

111. The RFS has the power to cancel or suspend a society from the Registry (section 6 of the Act), while the Minister may hold an inquiry or direct a person authorised by him/her to hold an inquiry in relation to the constitution, working and financial condition of a registered society. The Registrar, or any person authorised by the Registrar has unfettered access to all the books, accounts, papers and securities of a registered society, including information on the transactions and working of a friendly society (section 16 of the Act). Every registered society must keep books of account (section 11 of the Act) and must appoint an auditor approved by the Registrar to audit the society's accounts on an annual basis.

112. **Criterion 8.4** –

a) The Board of Charities and the RFS are responsible for monitoring charities' and friendly societies compliance with registration and accounting requirements. According to the CharA (section 6, par.8) and the Friendly Societies Act (section 19) the commissioners and the Registrar have sufficient powers to monitor and inquire charities and societies respectively.

b) The CharA (section 19, par.19) and the Friendly Societies Act (Section 6) provide a range of effective, proportionate, and dissuasive sanctions. In particular, the Commissioners may: of their own motion remove any trustee, charity trustee, officer, agent or servant of the charity; vesting in or transfer to the official custodian for charities of property held by or in trust for the charity; may order any bank or other person who holds money or securities on behalf of the charity or of any trustee for it not to part with the money or securities without their approval; and restrict the transactions which may be entered into, or the nature or amount of the payments which may be made, in the administration of the charity. Also, the Registrar may cancel or suspend the registry of a society. These sanctions do not preclude the imposition of criminal sanctions under POCA.

113. **Criterion 8.5** –

a) General reporting obligations for NPOs are in place. The majority of data regarding charities and friendly entities can be found in the Register of Charities and the RFS, which are accessible to the public. Exchange of certain relevant information between the Board of Charity Commissioners and any Government Departments is allowed through the CharA (section 11). Co-operation and co-ordination amongst appropriate authorities holding relevant information on NPOs is only taking

place on an informal basis. Both regulators do not hold any summits and do not form part of any inter-agency FT working group.

b) Investigations into the affairs of the activities of a charity known or suspected to be involved in FT activities would be performed by the money Laundering investigation unit (MLIU) of the RGP. There are no statutory impediments in doing so. The same powers are available with regard to friendly societies. Officers of the MLIU are trained to the UK National Crime Agency (NCA) financial investigators' standards. Also, three out of the four officers of the MLIU have also undergone FT-related training by the training UK National Terrorist Financial Investigation Unit (NTFIU).

c) Full information on the administration and management of particular NPOs is accessible in a timely manner, given that relevant information is stored publicly and is easily accessible (S.4 par.6(7) of the CharA and S.5(6) of the FSAct).

d) A person commits an offence if he does not disclose to a police constable (to be read as meaning GFIU) as soon as is reasonably practicable his belief or suspicion that another person has committed an FT offence (Terrorism Act 2018, s.40-47). In addition, where a supervisory authority, in the course of checks carried out on persons for whom it is the supervisory authority or in any other way, discovers facts that could be related to ML/FT, it shall promptly inform the GFIU (POCA s.30(A)). POCA (S.J(1)) also stipulates that in terms of internal cooperation there should be nothing to preclude or prevent the exchange of intelligence between the GFIU and the RGP and HMC or with the supervisory bodies.

114. **Criterion 8.6** – International requests for information regarding particular NPOs suspected of FT or involved in other forms of terrorist support are executed by the same contact points as exist for LEA to LEA, FIU to FIU, MLA or Egmont requests.

Weighting and Conclusion

115. There are legal instruments and procedures in place. However, there is no specific policy document on the promotion of transparency, no outreach or educational programmes to donors have been conducted. In addition, no NPOs were involved in the development and refinement of best practices to address FT risk and vulnerabilities, and the effective co-operation, co-ordination among all levels of appropriate authorities or organisations that hold relevant information on NPOs is not guaranteed. Overall, four criteria are met, one criterion mostly met and one partly met. **R.8 is rated LC.**

Recommendation 9 – Financial institution secrecy laws

116. In its 2007 IMF Report, Gibraltar was rated compliant with former R.4 (para. 2.4, p. 60). It was noted that there was no statutory secrecy law in Gibraltar and banking confidentiality in Gibraltar was governed by the general principle at Common Law as applicable in the United Kingdom, i.e., a bank owes a legal duty of confidentiality to its client arising out of a contract. However, this duty was not absolute, but qualified by over-riding duties, one of which was the duty of a bank to comply with the law.

117. **Criterion 9.1** – In its 2007 IMF Report, Gibraltar was rated C with former R.4. It was noted that there was no statutory secrecy law in Gibraltar and banking confidentiality in Gibraltar was governed by the general principle at Common Law as is applicable in the United Kingdom, i.e., a bank owes a legal duty of confidentiality to its client arising out of a contract. However, this duty was not absolute, but qualified by over-riding duties, one of which was the duty of a bank to comply with the law.

118. There are no financial institution (FI) secrecy laws that inhibit the implementation of all AML/CFT measures (including those under the FATF Recommendations) in Gibraltar. Common law sets out a bank's duty of confidentiality and states that there are four exemptions to an FI's duty to not disclose client information, including where disclosure is under exemption by law (i.e. under a court order or a statutory requirement to provide information) (Court of Appeal in *Tournier v National Provincial and Union Bank of England* [1924] applies in Gibraltar)⁹⁸. The *Tournier* Rules are applicable, for example, when making a pre-order enquiry with a bank (FI) to obtain information. The provisions under Sec 4G(5) of Proceeds of Crimes Act 2015 (POCA) provides that an authorised disclosure is not to be taken to breach any restriction on the disclosure of information (however imposed). Furthermore, there are provisions under Sec 4G(6) of POCA, that provides, where an authorised disclosure is made in good faith, no civil liability arises in respect of the disclosure on the part of the person by or on whose behalf it is made.

119. *Access to and Sharing of information by Competent Authorities:* The GFSC can provide to an authority of Gibraltar (in accordance with the list of authorities provided in the FS(IG&C)A) or to a similar supervisory authority outside of Gibraltar, any information received under Section 4(1) of the FS(IG&C)A. The powers of the GFSC include the possibility to compel and access any documents from relevant persons and firms and/or to make enquiries accordingly. Section 3 deals with data protection rules consistent with EU Regulations. However, the disclosure of information is not limited by data protection rules, as long as it is provided to another authority in Gibraltar or to a similar foreign counterpart.

120. Part III of the FS(IG&C)A includes the power of the GFSC to obtain information from firms as required. This part is applied by Section 12 of the same Act. Furthermore, Section 12 of the Act encompasses all the powers available to the GFSC in accessing information from firms to be used for the purposes of sharing information internationally or with a foreign authority.

121. Additionally, Section 12(1) of the FS(IG&C)A does not restrict the GFSC with regards to the type of information which can be obtained from firms as long as it is used for "*the purpose of assisting an authority*". Section 1DA(2) of POCA includes international cooperation and the applicability of such provision to all supervisory bodies, FIU and LEAs. Section 1K of POCA also provides the access to information held by the GFIU. Furthermore, nothing can prevent international cooperation under Section 1J of POCA.

122. *Sharing of information between FIs:* There are no FI secrecy laws or application of common law in Gibraltar that restricts the exchange of information between firms. The gateway to discuss this within a firm's Group is opened under Section 5(5) of POCA. This is also the case where it is required under R. 13, 16 and 17. Moreover, since the Wire Transfer Regulations (847/2015) came into force, all wire transfers between FIs must contain certain information regarding a customer's name, address and account number; this is particularly relative to R.16. In addition, Section 4G(5) of POCA reiterates that an "*authorised disclosure is not to be taken to breach any restriction on the disclosure of information (however imposed)*".

Weighting and Conclusion

123. **R.9 is rated C.**

⁹⁸ Section 2 of the English Law (Application) Act (<https://www.gibraltarlaws.gov.gi/articles/1962-080.pdf>) is the authority that provides that common law and the rules of equity from time to time in force in England shall be in force in Gibraltar, so far as they may be applicable to the circumstances of Gibraltar and subject to such modifications thereto as such circumstances may require.

Recommendation 10 – Customer due diligence

124. In 2007 IMF Report former R.5 was rated PC. Several criteria were not appropriately addressed in laws or regulations and instead were part of the Guidance Notes on systems of control to prevent the financial system from being used for ML or TF activities (Anti Money Laundering Guidelines - AMLGN), issued by the FSC, which at the time lacked the authority to issue such type of guidance. AMLGN have been re-issued by the FSC addressing the identified deficiency. Gibraltar has also revised relevant laws and regulations significantly rendering the analysis of former R.5 in the 2007 IMF Report obsolete. Requirements for FIs, which are included in the broader category of RFBs, to conduct CDD are now set in the Proceeds of Crime Act (POCA)⁹⁹ and in the AMLGN. As described in Chapter 1 POCA is the primary legislation. FI must comply also with requirements in AMLGN, which are considered as other enforceable means.¹⁰⁰

125. **Criterion 10.1** – Credit institutions (CIs) and FIs are prohibited from setting up anonymous accounts or passbooks for any new or existing customers (Section 22(3), POCA). A CI or FI which seeks to carry on business in Gibraltar must subject the owner and beneficiary of an already existing anonymous account or passbook to CDD measures as soon as possible and in any event, before such account or passbook is used in any way (Section 22(3A), POCA). AMLGN stipulates also that regulated firms should subject the owner and beneficiary of an existing anonymous account or passbook to CDD measures as soon as possible and in any event before such account or passbook is used in any way (Section 6.2.2.1). Firms may not permit their products (including account and passbooks) to be used applying obviously fictitious names or where the customer's name is not identified (R22, AMLGN).

126. **Criterion 10.2** – RFBs are required to apply CDD when, *inter alia*: (i) establishing a business relationship; (ii) when carrying out an occasional transaction amounting to 15,000 euro or more, whether the transaction is carried out in a single operation or in several operations which appear to be linked; (iii) when it suspects ML or TF, regardless of any derogation, exemption or threshold; (iv) when it constitutes a transfer of funds as defined by EU Regulation 2015/847 (WTR); or (v) when it doubts the veracity or adequacy of “*documents, data or information previously obtained for the purposes of identification or verification*” (Section 11(1), POCA). The extent of CDD measures to be applied should be determined on a risk-sensitive basis depending on the type of customer, business relationship, product or transaction (Section 11(3), POCA). Transactions that are separated by an interval of three months or more need not, in the absence of specific evidence to the contrary, be treated as linked (Section 6.2.2.7.1, AMLGN).

127. **Criterion 10.3** – Section 10(a) of the POCA provides the definition of CDD measures which comprise, *inter alia*, of: “*identifying the customer and verifying the customer's identity on the basis of documents, data or information obtained from a reliable and independent source*”. The definition is reiterated in the AMLGN which states that CDD should be performed whether the customer is a natural or legal person or legal arrangement (R59 and R60). There is no definition of ‘customer’ in POCA or AMLGN, therefore it is inferred that it includes both natural persons and legal entities, especially as AMLGN gives extensive details on the information and documents needed to perform

⁹⁹ RFB – Relevant financial business, defined by POCA (Section 9), includes Financial Institutions as defined by FATF.

¹⁰⁰ POCA provides that in deciding whether a person has committed an offence under POCA, the courts must consider whether that person followed any relevant guidance which was at the time issued by a supervisory authority or any other appropriate body (Section 33(2)). The guidance is meant to complement the legal provisions established by POCA, therefore, as confirmed by the authorities, they cannot establish new requirements or requirements that would go beyond what is stipulated by POCA. Within these boundaries, SBPR also states that a supervisory body may impose a sanction if there is a breach of any applicable law or guidance (Sections 18 to 21, SBPR).

identification and verification of the customer, separate for natural persons, bodies corporate and legal persons, trusts and similar legal arrangements (R71 to R90 of the AMLGN). In exceptional circumstances when potential customers are not able to provide appropriate documentary evidence of identity and independent address verification is impossible, a senior manager may nonetheless authorise the business (Section 7.2.2, AMLGN). Also, where the applicant for business is known to be a listed company no further steps to verify identity, over and above usual commercial practice, will normally be required (R6.2.1.2.1, AMLGN). Verification of identity is not required when there are *reasonable grounds for believing* that the applicant for business is itself a FI in Gibraltar or in EU country – which includes verifying that the CI or FI actually exist and that it is also regulated, inferring also a presumption that it is compliant with 4th AMLD (R6.2.1.2.2, AMLGN). The exceptions are not based on a proven low risk assessment (see Criterion 1.6 TCA).

128. **Criterion 10.4** – CDD measures include verifying that any person purporting to act on behalf of the customer is so authorized and identifying and verifying the identity of that person (Section 10A, POCA). Same is stated in AMLGN, which also provides that the extent of applying CDD measures shall be determined on a risk-sensitive basis (R60, recital (e), AMLGN).

129. **Criterion 10.5** – Identification of the BO is part of the CDD measures. The FI should take reasonable measures, on a risk sensitive basis, to verify BO's identity so that the FI is satisfied that it knows who the BO is (Section 10(b), POCA). AMLGN includes also the requirement to identify and verify the BO, applying the risk sensitive basis to its extent (R60(b)).¹⁰¹

130. **Criterion 10.6** – CDD measures include the *assessment* and, as appropriate, obtaining information on the purpose and intended nature of the business relationship (Section 10(c), POCA). Additionally, the AMLGN specifies that CDD measures include *understanding* and obtaining information on the purpose and intended nature of the business relationship (R60(c), AMLGN).

131. **Criterion 10.7** – RFBs are required to conduct on-going monitoring of a business relationship (Section 12(1), POCA). Section 12(2) of the POCA gives a definition of “*on-going monitoring*”, which is narrowed to “*the scrutiny of transactions undertaken throughout the course of the relationship (including, where necessary, the source of funds) to ensure that the transactions are consistent with the RFB's or person's knowledge of the customer, his business and risk profile, including where necessary the source of funds*”. The definition also requires RFBs to keep “*the documents, data or information obtained for the purpose of applying customer due diligence measures up-to-date*”. Firms are required to ensure that documents, data or information obtained is kept *relevant* (R60(f), AMLGN). There is a requirement to ensure that documents are kept up-to-date particularly for higher risk categories conducting on-going monitoring on a risk-sensitive basis (Section 12(3), POCA). However, there is no explicit requirement to undertake reviews of existing records to ensure that documents, data or information collected under CDD process is kept up-to date and relevant.

132. **Criterion 10.8** – CDD should comprise of, inter alia, in case of clients which are legal persons and legal arrangements, “taking reasonable measures to understand the ownership and control structure of the customer” (Section 10(b), POCA). The AMLGN reiterates the definition and provides for the requirement of all firms to understand fully the legal form and structure and ownership of their body corporate customers and document this understanding (R60 and R77). There is no explicit provision relating to understanding the nature of the business. However, there is an obligation for firms to pay special attention to any activity which they regard as particularly

¹⁰¹ However, some of the DNFBP's supervisory authorities (e.g. RSC) have understood this requirement as non-mandatory for the low risk customers; i.e. when applying simplified due diligence measures, there is no obligation to identify or verify the BO and to understand the purpose and nature of the business relationship (see IO4).

likely, by its nature, to be related to ML or FT (R95 AMLGN). In case of legal arrangements and trusts, the firms should obtain information on all parties involved (trustees, settlor, grantor, protector, beneficiaries) and on the nature and purpose of the trust (R82-R8, AMLGN).

133. **Criterion 10.9** – For customers that are legal persons or legal arrangements, the information required to perform CDD is stated in the AMLGN, i.e. RFBs should verify the identity of the customer through: a) name, legal form and proof of existence; b) the powers which regulate and bind that legal person or legal arrangement; c) the name of the relevant persons having a senior management position in the “company” (*but not also in the legal arrangement*); d) the address of the registered office and if different, a principal place of business (R60A, AMLGN).

134. **Criterion 10.10** – Definition of the BO is provided in Section 7(1A) to (1C) of the POCA and means either or both a natural person who ultimately owns or controls the customer and a natural person on whose behalf a transaction or activity is being conducted. While FATF Criteria 10.10 a) and b) institute a hierarchy of provisions for identifying the BO (*only when there is doubt on the person having controlled ownership or no-one can fit the criteria, can the financial institution identify as BO a person exercising control through other means*) the provisions in POCA do not consider such hierarchy. For example, owning a customer, controlling a customer through ownership or exercising control over the customer through other means are overlapping criteria. Section 7(1A)(i) of POCA defines BO for a legal entity as “*the natural person who ultimately owns or controls a legal entity through direct or indirect ownership of a sufficient percentage of the shares or voting rights or ownership interest in that entity, including through bearer shareholdings, or through control via other means*”. These requirements do not apply when a customer is listed on the regulated market and is subject to disclosure requirements (Section 7(1A)(a)(i), POCA and R61, AMLGN), in line with FATF standards. The definition in POCA considers the relevant provisions of EU Directive 2015/849 which institutes a threshold of shareholding of 25% plus one share or an ownership interest of more than 25% in the customer as an indication of direct ownership (Section 7 (1B), POCA). The Minister may, by legal notice in the Gazette amend the percentage referred to in sub-section 7 (1B) of the POCA which may be taken as an indication of ownership or control (by the time of the assessment none have been issued). If, after having exhausted all possible means and provided there are no grounds for suspicion, no person is identified under the provisions above, or if there is any doubt that the person identified is the BO, the natural person who holds the position of senior managing official is identified as BO (Section 7(1A)(ii), POCA). AMLGN indicates also the information that should be collected in case the application of business is made in the name of a club or society. Apart from name, legal status and purpose, a firm should also obtain the identities of the officers of a club or society who have authority to operate an account or to give instructions concerning the use or transfer of funds or assets (Section 7.7.1.7, AMLGN).

135. **Criterion 10.11** – Definition of the BO for trusts and other legal arrangements is provided in Subsection 7(1A) and 7(1B) of the POCA. A similar definition of BO is given in R61 of the AMLGN. In relation to trusts, firms should obtain: a) full name of the trust; b) nature and purpose of the trust (e.g., discretionary, testamentary, bare); c) country of establishment; d) identity of the settlor or grantor; e) identity of all trustees; f) identity of any protector; g) where the beneficiaries have already been determined, the identity of the natural person(s) who is the beneficial owner of 25% or more of the property (*and not on all beneficiaries, as required by FATF*); h) where the individuals that benefit from the legal arrangement have yet to be determined, the class of persons in whose main interest the arrangement is set up.

136. **Criterion 10.12** – CIs or FIs involved in life insurance or other investment-related insurance activities should conduct additional CDD measures on the beneficiary of the life insurance, as soon as the beneficiary is identified or designated: a) for a beneficiary that is identified as specifically named natural or legal persons or legal arrangements, taking the name of the person; b) for a

beneficiary that in the case of beneficiaries that are designated by characteristics or by class or by other means, obtaining sufficient information concerning those beneficiaries to satisfy the CI or FI that it will be able to establish the identity of the beneficiary at the time of the pay-out. The verification of the identity of beneficiaries shall take place at the time of the pay-out (Section 13(4A), POCA).

137. **Criterion 10.13** – There is no explicit provision in POCA for the beneficiary of a life insurance product to be considered as a risk factor when determining whether EDD are applicable (Section 26(2A), POCA). Nevertheless, there is a general provision for FIs to take into consideration customer risk factors in deciding whether to apply EDD. (Section 17(4) of POCA)

138. **Criterion 10.14** – As a general rule, RFBs are required by law to verify the identity of the customer and the BO before establishing a business relationship or conducting occasional transactions (Section 13(2), POCA). In case of establishing business relationships, verification can be completed during the establishment, provided that: (a) this is necessary not to interrupt the normal conduct of business; and (b) there is little risk of ML/FT (Section 13(3), POCA). Secondly, FIs may complete verification after an account has been opened if there are adequate safeguards in place to ensure that no transactions are carried out by (or on behalf of) the customer before verification has been completed (Section 13(5), POCA). In case of transactions, where satisfactory evidence of identity is required, a firm should "freeze" the rights attaching to the transaction pending receipt of the necessary evidence. The customer may continue to deal as usual, but, in the absence of the evidence of identity, proceeds should be retained. Documents of title should not be issued, nor income remitted, but may be re-invested (Section 7.2.1 AMLGN).

139. **Criterion 10.15** – There is no explicit requirement that RFBs should adopt risk management procedures concerning the conditions under which a customer may utilize the business relationship prior to verification. However, the legislation does not permit the completion of verification after utilising the business relationship. Bank accounts cannot be closed, and no transactions can be carried out by or on behalf of the account holder until the identity of the holder of the bank account has been verified (Section 13(5), POCA). In case of transactions, AMLGN institutes certain provisions regarding freezing of assets. (see C.10.14). There is also a general requirement for developing relevant risk management policies and procedures (Section 26(1), POCA).

140. **Criterion 10.16** – RFBs should apply CDD measures at other appropriate times to existing customers on a risk-sensitive basis, including at times when the relevant circumstances of a customer change (Section 11(2), POCA; R68, AMLGN). However, there is no explicit requirement to consider *the materiality* as required in the standards.

141. **Criterion 10.17** – RFBs are required to apply EDD measures in cases underlined in Art 19 to 24 or the EU Directive 2015/849 (Section 17(1)(a), POCA). EDD measures must be applied for complex and unusual transactions, when dealing with customers established in third countries identified by the European Commission as high risk third countries (Section 17(1)(b), POCA). RFBs are required to consider NRA findings and apply EDD measures when offering a product or service which is identified as a high risk (Section 25A, POCA). EDD measures must be also applied whenever the RFB or the Minister (under the condition on notice in the Gazette) identifies higher risks (Section 17(1)(c), POCA). Specifically, a RFB must examine, as far as reasonably possible, the background and purpose of all complex and unusually large transactions, and all unusual patterns of transactions, which have no apparent economic or lawful purpose; in particular, a RFB shall increase the degree and nature of monitoring of the business relationship, in order to determine whether those transactions or activities appear suspicious (Section 17 (3), POCA). A non-exhaustive list of factors for determining the level of risk is given in Schedule 7 of the POCA, which

reproduces Annex III of the EU Directive 2015/849. Also, the AMLGN provides a list of situations when EDD measures must be applied (Section 6.2.2.8, AMLGN).

142. **Criterion 10.18** – RFBs may apply simplified CDD when it identifies areas of lower risk and has ascertained that the relationship or the transaction presents a lower degree of risk (Section 16(1), POCA). A list of risk factors that a RFBs must consider is provided in Schedule 6 of POCA and includes some that are not based on a country assessment of risk (for example residence in an EU member state.) Derogations from the need to undertake sufficient monitoring of the transactions and business relationships to enable the detection of unusual or suspicious transactions are not permitted (Section 16(2), POCA). RFBs are required also to consider the NRA findings (Section 25A, POCA). Irrespective of the size and nature of the transaction or customer, reduced due diligence measures should not be applied where ML or TF is known, believed or suspected. As well, where higher risk scenarios or factors apply, a payment service provider should not apply reduced due diligence measures (Section 6.2.2.7, AMLGN).

143. **Criterion 10.19** – RFBs are required not to establish a business relationship, to terminate any existing relationship or it should not carry out an occasional transaction for which the required CDD could not be performed (Section 15(1), POCA). As regards to accounts, there are no explicit provisions that prohibit the opening of such accounts for which CDD has not been performed, instead it is stipulated that no transaction should be carried through that account (Section 15(1)(a), POCA). In relation to filing an SAR, RFB must consider whether, given all the information at hand and consideration, it should make a report (Section 15(1)(b), POCA).

144. **Criterion 10.20** – There is a general requirement for RFBs to file a disclosure to GFU whenever it forms a suspicion or knowledge of ML or FT (Section 6B, POCA). There is no explicit permission not to pursue the CDD process if it is believed this might tip-off the customer. The AMLGN provides that where a firm is unable to complete its CDD measures because it has formed a suspicion or knowledge of ML or FT and completing the process is likely to tip-off the customer, it is expected to make a disclosure to the GFU in line with Section 6B of the POCA (introduction and Section 7, AMLGN).

Weighting and Conclusion

145. While a large part of the CDD measures meet the FATF standards, some minor deficiencies remain. Exceptions from the general rule of CDD requirements are not entirely in line with standards as they are not based on an assessment of risk. There is no explicit requirement to undertake reviews of existing records to ensure that documents, data or information collected under CDD process is kept up-to date and relevant and to understanding the nature of the business. The legal requirement to verify the identity of the customer for customers that are legal persons or legal arrangements does not include for legal arrangements the obligation to obtain the name of the relevant persons having a senior management position. The requirements of identification of the BO do not follow the hierarchy of provisions in the standards. In case of legal arrangements, only beneficiaries that hold more than 25% of the property are required to be identified. There are no explicit provisions for the beneficiary of a life insurance product to be considered as a risk factor when determining whether EDD are applicable and to consider *the materiality* when applying CDD requirements to existing customers. Guidance on lower risks in relation to EU members is not based on an assessment of risk and there are no explicit provisions that prohibit the opening of accounts for which CDD has not been performed. Additionally, there is no explicit permission not to pursue the CDD process if it is believed this might tip-off the customer. **R.10 is rated LC.**

Recommendation 11 – Record-keeping

146. Gibraltar was rated PC for former R.10 in the 2007 IMF Report. The deficiencies included the absence of requirements for retaining business correspondence and maintaining the records in a way that FIs can provide information to the appropriate authorities on a timely basis when appropriately authorised to do so.

147. **Criterion 11.1** – The record keeping requirements are stipulated in the POCA (S25, POCA) and AMLGN (R108), which includes a list of records, which RFBs are expected to retain at minimum. RFBs are required to maintain the supporting evidence and record of transactions (original documents and copies) necessary to identify transactions for a minimum of five years from the time the occasional transaction is completed, the business relationship ends or, in case of records that relate to a particular transaction, the date on which the transaction is completed (Section 25(1), (2) and (3), POCA). Under the POCA, record keeping measures are required only for those business relationships and occasional transactions for which CDD or on-going monitoring is required (Section 25(2)(b) of POCA). Therefore, not all types of transactions are covered (e.g. occasional transactions below the threshold of EUR 15.000 are not covered). Nevertheless, requirements of C.11.1 are broadly covered by accounting provisions which demand for the retention of records on transactions for a period of 6 years (Financial Services (Accounting and Financial) Regulations, Section 4 and 10). RFBs are permitted to rely on a third party including for record keeping obligations, provided that the third party is regulated and supervised. However, the RFB remains liable for any failings to apply existing measures (Section 23(1) of POCA). No distinctions are drawn between domestic and international transactions.

148. **Criterion 11.2** – RFBs are required to keep a copy of the documents and information relating only to the *customer's identity*, and not more generally to all records obtained through CDD measures. These documents do not expressly include information on the BO¹⁰² (Section 25 (1), (2) and (3), POCA). An implicit obligation to keep records (including in relation to the BOs) can be inferred by R106 of the AMLGN, which requires records to be prepared and maintained so as to permit a swift response to enquiries from court or LEAs requesting information, *including all CDD information*. Firms are obliged to maintain “*relevant records*” (Section 10.2 of the AMLGN), which include records on notes, email exchanges and correspondence. The requirement to retain records on any analysis undertaken by the firm is stipulated in AMLGN (R106(d), AMLGN). Additionally, there is no explicit provision in POCA to keep account files. However, AMLGN includes requirement to keep details on accounts, when those are used for payments (R108, AMLGN).

149. **Criterion 11.3** – According to the POCA, RFBs must keep supporting evidence and records of transactions (original documents or copies) necessary to *identify* transactions (Section 25(2)(b)), rather than to allow transactions to be reconstructed. AMLGN specifies that records must be kept as to allow that any transactions effected via the institution can be reconstructed in such a manner as to provide evidence for prosecution of criminal activity, if necessary (R106(c), AMLGN). There is a timeframe of 5 years instituted for record keeping with a longer period for

¹⁰² According to this provision, the records that should be kept are “*a copy of, the documents and information which are necessary, the evidence of the customer's identity*”. These documents are identified with a very specific cross reference to other sections of POCA, i.e. “sections 10A, 11, 12, 13, 14, 16, 17, 17A, 18, 19, 20, 20B or 22(3)”. In this specific cross reference to measures, however, there is no mentioning of Section 10, which is the provision that specifies the CDD measures, including 10 (b), which requires RFB to obtain and take reasonable measures to verify the BO's identity. Therefore Section 25 of POCA, by referring only to the ‘*customer's identity*’ and by not making any reference to the BO, could be interpreted to exclude from the record keeping requirement documents related to the BO. Especially as POCA utilizes the expression “*customer's identity*” distinguishing it from “*BO's identity*”, particularly when defining the CDD measures in section 10, and in other parts of POCA (e.g. in case of third-party reliance).

information related to legal proceedings which commenced prior to 25 June 2015, where this information be kept until 25 June 2020 (subject to the GDPR) (Section 25ZA, POCA). Where a firm has submitted a suspicious transaction report to the GFIU or where it knows that a client or transaction is under investigation, it should not destroy any relevant records without the agreement of the authorities even though the five-year limit may have been reached (R100 of the AMLGN).

150. **Criterion 11.4** – RFBs are required to “*have systems in place which allow for full and speedy responses to a request*” from the GFIU, law enforcement authorities or supervisory authorities about whether the RFB has maintained a business relationship with the person in question in the 5 years prior to the request (Section 30B (1), POCA). Firms must prepare and maintain records so that an enquiry or court order from the authorities can be responded to swiftly. This includes all CDD information and transaction records (R106 (e), AMLGN) but this principle should be set out in law. In addition, Financial Services (IG&C) Act 2013 allows the GFSC to obtain any information and share this with the domestic authorities should it be deemed necessary. (Part III, FS(IG&C) Act).

Weighting and Conclusion

151. The record keeping requirements concerning records obtained through CDD measures provided by the law are only limited to the customer’s identity. Reference to other documents obtained through CDD measures, including the BO, appear to be only implicit and are included in other enforceable means. Additionally, there is no direct requirement to keep records on account files, but only accounts details when those are used for payments. **R.11 is rated PC.**

Recommendation 12 – Politically exposed persons

152. **Criterion 12.1** – There is no distinction in Gibraltar legislation between foreign and domestic/international PEPs, therefore, these are treated in the same manner and the analysis below applies to all types of PEPs. The definition of a PEP is provided by section 20A of POCA, which considers the list provided by EU Directive 2015/849 and is in line with the FATF definition. Section 20A of the POCA also provides definitions for “*family members*” and “*persons known to be close associates*”. In deciding whether a person is a known close associate of a PEP, FIs need only have regard to information which is in its possession or is publicly known (e.g. 3rd party databases). Section 20B of the POCA sets out that for at least 12 months from the time a customer is no longer entrusted with a prominent public function, the RFBs must consider the continuing risk posed by that person and apply appropriate and risk sensitive measures (until that person is deemed to pose no further risk specific to PEPs).

(a) Risk management systems: RFBs must have appropriate and risk-sensitive policies, controls and procedures to determine whether a customer, or a BO of a customer, is a PEP, by way of the provision of appropriate risk management systems, including risk-based procedures (Section 26(2)(c), POCA; R20(b), AMLGN). Nevertheless, some authorities¹⁰³ have interpreted this requirement in the way that not all customers must be checked whether they are PEPs and instead checks can be done selectively on a risk-sensitive basis.

(b) Obtaining senior management approval: RFBs that propose to have a business relationship with a PEP must, in addition to normal CDD measures, have approval from senior management for establishing or continuing the business relationship with that person. There is no specific provision for obtaining senior management approval if the BO of the customer is a PEP (Section 20(1)(a) of POCA; R20(c) of the AMLGN).

¹⁰³ RSC

(c) Establish the source of wealth and source of funds: RFBs that propose to have a business relationship or carry out an occasional transaction with a PEP must, in addition to normal CDD, take adequate measures to establish the source of wealth and source of funds which are involved in the business relationship/occasional transaction. This provision does not cover customers already onboarded at the time of the adoption of POCA (Section 20(1)(b), POCA 2015).

(d) Conduct enhanced on-going monitoring: In addition to the CDD, where the business relationship with a PEP is entered, RFBs must conduct enhanced on-going monitoring of the relationship. (Section 20(1)(c), POCA). RFBs have the obligation to establish and document a clear policy and internal guidelines, procedures and controls regarding business relationships with PEPs and those business relationships which are known to be related to PEPs must be subject to proactive monitoring of the activity on such accounts. The monitoring of the accounts is necessary so that any changes are detected, and consideration can be given as to whether such change suggests corruption or misuse of public assets given the relation to the PEP (S20(1)(c), POCA; R20(a) and (d), AMLGN).

153. **Criterion 12.2** – There is no distinction in Gibraltar legislation between foreign and domestic PEPs, therefore, the requirements for domestic and foreign PEPs have been addressed in the previous Criterion.

154. **Criterion 12.3** – The obligation to have policies and procedures to determine if a customer/BO is a PEP does not extend to family members or persons known to be close associates of PEPs. Only the provisions in relation to senior management approval, establishing the source of wealth/funds and conducting enhanced on-going monitoring apply to family members and close associates (Section 20(2), POCA). Given the shortcoming identified in Criterion 12.1, the cases where the BO of the customer is a family member, or a close associate of a PEP are not properly addressed by the legislation (Section 20(2), POCA). They are partially touched upon in the guidelines, which states that EDD must also applied for PEPs, family members and close associates of PEPs, whether they be as a customer or BO (Section 6.2.2.8 of AMLGN).

155. **Criterion 12.4** – Policies and procedures determining if a beneficiary of a life insurance product (or BO of the beneficiary) is a PEP should be implemented no later than at the time of the pay-out or the assignment, in whole or in part, of the policy (Section 26(2A), POCA). Further, where higher risks are identified, in addition to CDD, RFBs must ensure that senior management is informed before pay-out of policy proceeds and conduct enhanced scrutiny of the entire business relationship with the policyholder (Section 26(2A), POCA). The consideration for making a suspicious transaction report is covered by Section 15(1)(d) of the POCA, in cases where CDD cannot be conducted. The requirement to file a disclosure is also addressed under Section 6B of the POCA where a SAR must be filed where there is knowledge or suspicion of ML or FT.

Weighting and Conclusion

156. Several shortcomings have been identified. Given the wording of the POCA and explanations provided by the authorities, determining whether the client is a PEP is not mandatory for all customers, but it can be interpreted as based on a risk sensitive approach. There is no clear provision for obtaining senior management approval if the BO of a client is a PEP or for implementing policies or procedures to determine if the customer/BO is a family member or close associate of a PEP. Requirement to establish the source of wealth and source of funds is not mandatory for already existing PEP customers. **R. 12 is rated PC.**

Recommendation 13 – Correspondent banking

157. Gibraltar was rated LC for former R.7 in the 2007 IMF Report. Some deficiencies were identified regarding the need to ensure that information has been gathered on respondents, to understand fully the nature of the respondent’s business and to determine whether it has been subject to any actions related to AML/CFT. Overall, the correspondent banking relationships in Gibraltar were extremely limited and it was more feasible for most Gibraltar banks to route payments through the parent bank, rather than setting up their own correspondent relationships.

158. **Criterion 13.1** – The legal provisions regarding correspondent banking relationships only apply if the respondent institution is from a non-EEA State or Territory (or outside the EU). Sections 19(a) to (d) and 17A of the POCA and Section 6.2.2.8.1 of the AMLGN follows the provision of Criterion 13.1 for correspondent relationships and other similar relationships (as defined under Section 7(1) of the POCA) including the requirements to: gather sufficient information to understand the nature of the respondent’s business, to determine the reputation of the institution and the quality of supervision, including whether it has been subject to a ML/FT investigation or regulatory action; assess the respondent institution’s AML/CFT controls; obtain senior management approval prior to establishing the relationship; and clearly understand and document the respective responsibilities of each institution.

159. **Criterion 13.2** – Sections 17A(1)(e) covers requirements with respect to payable-through accounts and 19(f) of the POCA covers requirements in respect of customers who have direct access to accounts of the correspondent. The provisions apply when the respondent is not based in an EEA State or Territory. The respondent institution must identify and verify the identity of its customers, applying all CDD measures as stated in Section 17A(1) of the POCA which makes direct reference to the CDD requirements within Article 13 of the 4th AMLD. Also, R24 of the AMLGN requires that firms verify the verification conducted by the respondent institution. A CRFB has to ensure that the respondent “*is able to provide relevant CDD data to the correspondent institution, upon request*” (Section 19(f), POCA; R24, AMLGN). Additionally, firms must terminate the accounts of correspondents who fail to provide satisfactory answers to reasonable enquiries (R25 of the AMLGN).

160. **Criterion 13.3** – A CI or FI must not enter into or continue a correspondent banking relationship with a shell bank and must take appropriate measures that it does not enter into or continue a correspondent banking relationship with a bank “which is known” to permit its accounts to be used by a shell bank (rather than “satisfy itself” that the accounts of the respondent are not used by shell banks) (Section 22 of POCA).

161. POCA defines shell banks as credit institutions or FIs, or an institution that carries out equivalent activities, incorporated in a jurisdiction in which it has no physical presence, involving meaningful decision making and management, and which is unaffiliated with a regulated financial group (Section 22 (4) of POCA).

Weighting and Conclusion

162. While most criteria are met, they apply only to non-EEA countries and territories, which is not in line with FATF Standards. **R.13 is rated PC.**

Recommendation 14 – Money or value transfer services

163. Gibraltar was rated NC for former SR VI in the 2007 IMF Report, for the lack of overall framework in place. As with all money transmitters (excluding those housed in banks), alternative remittance providers were not subject to any licensing or registration requirements at the time.

Also, principals did not keep lists of all agents of money and value transfer service (MVTS) providers and there was no mechanism to ensure that money and value transfer service providers can be sanctioned.

164. **Criterion 14.1** – MVTS are licensed and regulated in Gibraltar through FS(IFS)A and FS(PS)R. MVTS providers are: currency exchange offices, which provide, *inter alia*, cash based foreign exchange and cashing cheques, buying/selling/exchanging of precious metals (but not precious stones); money transmitters and payment service providers (PSPs). All these activities are required to be licensed (Sections 3(1) and 3(2), FS(IFS)A). Additionally, the provision of MVTS via a CI or e-money institution (which would fall within their license permissions) is caught within the authorisation that is required to be obtained under the Financial Services (Banking) Act 1992 (Section 7(1), Schedule 1). As confirmed by the authorities, natural persons are not permitted to carry out MVTS activities under the legislation of Gibraltar.

165. PSPs must be authorised as payment institutions (PIs) according to FS(PS)R (Section 12(1)), transposing EU PSD2 (Directive (EU) 2015/2366). However, the exemptions indicated under Regulation 12(2) and referred to under Regulation 2(2)(c) to (g) are not applicable as these activities are captured through another type of authorisation such as a CI, e-money institutions or currency exchange offices. According to Section 32(1) there is the general exemption (in accordance with the PSD2) given by way of regulations, by the Minister, for small PIs. Nevertheless, up to the time of the onsite, none has been issued.

166. **Criterion 14.2** – Providing MVTS without a license constitutes an offence according to the FS(IFS)A and FS(PS)R. The GFSC, which undertakes the licensing and supervision of MVTS providers, carries out an analysis and requests information from firms in case it suspects MVTS activity, to ensure authorisation of such activity or ceasing it immediately.

167. Under Section 48 of FS(IFS)A the sanction is either: i) a conviction on indictment, prison up to 7 years or a fine, or both; or ii) summary conviction, a fine not exceeding GBP 25,000. Under Regulation 37 of FS(PS)R the sanction is a summary conviction of imprisonment not exceeding 3 months and/or a fine not exceeding level 5 on the standard scale. The standard scale refers to Schedule 9 of the Criminal Procedure and Evidence Act 2011 and a level 5 fine is to the amount of GBP 10,000. MVTS provider that is carrying on business without authorisation, may also be sanctioned under the SBPR. Additionally, Section 56(1)(e)(ii) of the Insolvency Act 2011 and Section 25(1)(a) of the Financial Services Commission Act 2007 allow the GFSC and Minister to make an application for a Court Order to liquidate or put the company into administration where it is identified that a company is conducting licensed activity without the relevant authorisation to do so.

168. **Criterion 14.3** – The POCA encompasses investment business and controlled activities under FS(IFS)A, exchange offices and the general activity of money transmission/remittance offices. Therefore, these activities fall under POCA and are supervised by the GFSC (Section 9(1), POCA).

169. **Criterion 14.4** – Currency exchange offices and money transmitters (as defined in FS(IFS)A) are not permitted to have agents or passport its services since passporting is regulated by the relevant EU Directives and they are not covered by relevant EU legislation. Therefore, Criterion 14.4 is not applicable for them. In relation to PIs, those who intend to provide services through agents must apply for approval from the GFSC. The GFSC has 2 months to inform the PI whether the agent has been registered or refused. Until the GFSC has registered the agent, the agent cannot undertake any relevant business. The PI has also obligation to inform the GFSC without undue delay of any changes regarding its use of any agent or any entity to which PI has

outsourced its activities (Section 18(1) to (7), FS(PS)R). The GFSC is required to maintain information on the agents in its register (Regulation 5(1), S(PS)R).

170. **Criterion 14.5** – This criterion is not applicable to currency exchange offices because they are not permitted to have agents. In relation to PIs, there is no explicit provision in the legislation requiring the inclusion of agents in the AML/CFT programs or for monitoring the agents. Nevertheless, PIs are required to provide GFSC with the internal control mechanisms that the agent will use in order to comply with its obligations in relation to ML and FT under the 4th AMLD (Section 18(1)(c), FS(PS)R). Therefore, whereas there is no relevant requirement in verbatim, the agent is required to have internal controls compliant with 4th AMLD.

Weighting and Conclusion

171. There is no explicit requirement for MVTs to include agents in their AML/CFT programs or monitor them. **R.14 is rated LC.**

Recommendation 15 – New technologies¹⁰⁴

172. In 2007, new technologies in Gibraltar were mentioned in AMLGN and addressed internet services and telephone banking. There was no general statement about other technologies. Former R.8 was rated PC in the 2007 IMF Report due to the lack of implementation of new language on non-face-to-face and new technologies for all institutions and lack of oversight for currency exchange offices, the Gibraltar Savings Bank, and money transmitters on these issues.

173. **Criterion 15.1**– Gibraltar has included prepaid cards and virtual currencies into its NRA. Furthermore, since 2018, any distributed ledger technology (DLT) related activity for storing or transmitting value belonging to others, needs to be authorised by the GFSC and DLT providers have to comply with POCA and the AMLGN. Furthermore, the GFSC issued additional Guidance Notes relating to DLT, specifically covering financial crime.

174. At FI level, when assessing the risks of ML/FT in order to decide the level of CDD measures applied, RFBs must take into account a list of non-exhaustive factors, among which new products and new business practices, including new delivery mechanisms, and the use of new or developing technologies for both new and pre-existing products (Section 17(4) and Schedule 7, POCA).

175. **Criterion 15.2** – There is general provision in POCA requiring RFBs to take appropriate steps to identify and assess the risks of ML and TF considering risk factors including those relating to their customers, countries or geographic areas, products, services, transactions or delivery channels. (Section 25A (1) of POCA). R21 of the AMLGN requires firms to undertake a risk assessment for new products, business practices, delivery mechanisms and developing technologies (for both new and existing products) prior to the launch of these. Consequently, firms must take appropriate measures to manage and mitigate the risks.

Weighting and Conclusion

176. All criteria are met. **R.15 is rated C.**

¹⁰⁴ The FATF revised R.15 in October 2018 and its interpretive note in June 2019 to require countries to apply preventive and other measures to virtual asset service providers and virtual asset activity. This evaluation does not assess Gibraltar compliance with revised R.15 because, at the time of the on-site visit, the FATF had not yet revised its assessment Methodology accordingly. Gibraltar will be assessed for technical compliance with revised R.15 in due course, in the context of its mutual evaluation follow-up process.

Recommendation 16 – Wire transfers

177. Gibraltar was rated LC for former SR VII in the 2007 IMF Report. It was identified that the level of application of the standards by the stand-alone money transmission agent was unknown given the lack of overall regulatory framework for these entities. At present, at the EU level, there is a Regulation 2015/847 (WTR) covering wire transfers, which reflects FATF standards. The WTR has direct application in all EU states and also applies to Gibraltar.

178. **Criterion 16.1** – For the purposes of WTR, domestic wire transfers are all transfers where the entire payment chain is located inside the EU in accordance with Footnote 42 of the 2013 FATF Methodology. The information a cross border wire transfer has to include from the PSP point of view is: (a) the required and accurate originator information (name, account number, address, official personal document number, customer ID number or date and place of birth), and (b) beneficiary information (name and account number). If the transaction is not made from/to a payment account, a unique transaction identifier is required rather than the account number (Art.4(1), (2) and (3), WTR). Before transferring funds, the payment service provider of the payer shall verify the accuracy of the information referred to in paragraph 1 on the basis of documents, data or information obtained from a reliable and independent source. (Art. 4(4), WTR)

179. **Criterion 16.2** – Article 6 of WTR provides for the information needed in batch files transmitted outside the Union (cross-border) and is consistent with FATF requirements.

180. **Criterion 16.3** – All cross-border transfers below EUR 1,000 are required to be accompanied by the required originator and beneficiary information (Art. 6(2)), WTR).

181. **Criterion 16.4** – Article 6 of WTR provides for situations where, even in the case of exemption, where there is a suspicion of ML/FT or the funds are transferred in cash or in anonymous account, the service provider of the payer must verify the information on the payer.

182. **Criterion 16.5 and 16.6** – Articles 5 and 14 of the WTR provide for the information that has to accompany domestic wire-transfers (where all the parties of the chain are located in EU). This is also covered by R31 and R30 of the AMLGN respectively. According to Article 14, PSPs shall respond fully and without delay to enquiries from authorities responsible for AML/CFT in other member states. R106 of the AMLGN requires firms to respond swiftly to any enquiries or court orders from the appropriate authorities as to disclosure of information, including all CDD information and transaction records. A wire transfer is also considered a transaction; therefore, this requirement must be complied with in providing law enforcement agencies or similar, with the relevant information without delay.

183. **Criterion 16.7** – Article 16 of the WTR provides for the obligation of the payment service providers to retain the records of the transactions for a period of 5 years. After this period, the information must be deleted, unless otherwise provided by national law.

184. **Criterion 16.8** – Article 4 (6) of the WTR provides that until full compliance with ensuring that the transfer is accompanied by the required information on the payer and payee, the payer's service provider shall not execute the transfer.

185. **Criterion 16.9** – Article 10 of the WTR provides that intermediary payment service providers shall ensure that all information received on the payer and the payee that accompanies a transfer of funds is retained with the transfer.

186. **Criterion 16.10** – The WTR does not provide for the exemption specified in this criterion regarding technical limitations and therefore this is not applicable in Gibraltar.

187. **Criterion 16.11** – Article 11 of the WTR provides for intermediary PSP to implement effective procedures, including, where applicable, ex-post or real time monitoring (but it must include one of these), in order to detect whether information on the payer or the payee is missing.

188. **Criterion 16.12** – Article 12 of the WTR provides for the obligation of the intermediary PSP to establish risk-based procedures for determining whether to execute, reject or suspend a transfer of funds lacking required payer and payee information. Also, it provides for some follow up action.

189. **Criterion 16.13** – Article 7 of the WTR provides for the obligation of the beneficiary PSP to implement effective procedures including, where appropriate, ex-post or real-time monitoring, in order to detect whether required originator or required beneficiary information in a transfer of funds is missing.

190. **Criterion 16.14**– Article 7(3) of the WTR provides for the obligation of the beneficiary’s payment service provider to verify the beneficiary’s identity, if the identity had not been previously verified. Article 16(1) of the WTR provides for the obligation to retain the information for 5 years.

191. **Criterion 16.15** – Article 8 of the WTR provides for the obligation of the beneficiary payment service provider to establish risk-based procedures for determining whether to execute, reject or suspend a transfer of funds lacking required payer and payee information. Also, it provides for some follow up action.

192. **Criterion 16.16** – The WTR is binding for all MVTs providers and, as per to its Art.2, applies to the transfers of funds, in any currency, which are sent or received by an ordering, intermediary or beneficiary FI established in the EU. PIs are required to provide GFSC with the internal control mechanisms that the agent will use in order to comply with its obligations in relation to ML and FT under the 4th AMLD, therefore, the agent is required to have internal controls compliant with 4th AMLD. (Section 18(1)(c), FS(PS)R).

193. **Criterion 16.17** – Article 9 and Article 13 of the WTR provide that the intermediary service provider and the beneficiary’s PSP (not the payer’s service provider) should consider missing or incomplete information on the payer of the payee (rather than all information) when assessing if a transaction is suspicious and whether it is to be reported to the FIU. Nevertheless, AMLGN indicates that when a PSP acts for both the payer and the payee it should take into account all information from the payer and the payee parties in order to determine whether disclosure to the FIU is required and also, if applicable, file a report in any country affected and make information available to the GFU.(R34C, AMLGN)

194. **Criterion 16.18** – R34D of the AMLGN requires MVTs providers to take freezing action and comply with prohibitions from conducting transactions with designated persons and entities, as per obligations set out in the relevant UNSCRs relating to the prevention and suppression of terrorism and TF and their successor resolutions.

Weighting and Conclusion

195. All criteria are met. **R.16 is rated C.**

Recommendation 17 – Reliance on third parties

196. Gibraltar was rated PC for the former R.9 in the 2007 IMF Report. Deficiencies identified included: FIs relying on intermediaries were not obtaining immediately from the intermediary information on the identity of the customer; BO of the account and the legal status of legal persons or arrangements and BO requirements were not included in law or regulation; FIs did not have access, without delay, to the identification or other relevant documentation housed with the

intermediaries; and there were no requirements for the ultimate responsibility for customer identification and verification to remain with the FI relying on the third party.

197. **Criterion 17.1** – The reliance on third party providers is not limited to CDD measures but also extends to record keeping requirements (Section 23, POCA). RFBs may rely on a third party if the third party is RFB authorised in Gibraltar or outside Gibraltar subject to holding equivalent AML/CFT standards and are authorised by an equivalent competent authority.

a) In relation to obtaining the necessary information relating to CDD from the third party, POCA includes following approaches (Sections 25(5) and (6), POCA):

- When the third party is authorised or supervised in Gibraltar, the obligation to provide CDD information/documentation falls directly onto the third party, as they are already licensed in Gibraltar and authorities consider that supervisory powers to impose compliance over the third entity are much wider and more effective.
- When the third party carries on business in another country, the RFB who is reliant must take steps to ensure that the third party will provide information and copies of documentation as needed. The onus here is placed on the regulated firm in Gibraltar to apply these measures as the third-party provider is not based locally and the powers of authorities would not extend to them unless these are providing services in Gibraltar on a passporting regime basis.

b) Regarding the timing, information/documentation must be submitted “*as soon as reasonably practicable*” (Section 25(5) and (6), POCA) and “*without delay*” in cases of occasional transactions introduced by overseas third parties (R48, AMLGN).

c) In respect to satisfying themselves that the third party is regulated and supervised accordingly, RFBs need only have “*reasonable grounds to believe*” that the standards are met (Section 23(1) of the POCA). The RFB remains liable for any failure to apply CDD and record-keeping measures by the third-party provider (Section 23(1)(b), POCA).

198. **Criterion 17.2** – Reliance on third parties established in a high risk third country is not permitted¹⁰⁵ (Subsection 23(1A) and (1B), POCA). RFBs may only rely on a third party provided that either the party is an authorised person in Gibraltar, carries business in another EEA state (and is assumed to be subject to the provisions of 4th AMLD), or is a person who carries business in a third country, as long as the legal provisions and supervision are equivalent to the requirements of 4th AMLD (Section 23(2)(c) and (d), POCA). No other information of the level of country risk is required to be considered by FIs, apart from reference to the EEA.

199. **Criterion 17.3** – RFBs are considered compliant with reliance provisions as long as the third party is part of the same group, the group applies CDD, record keeping and programs against ML/FT in accordance to POCA or equivalent rules (although there is no explicit provision for ensuring any higher country risk is adequately mitigated by the group’s AML/CFT policies) and is so supervised at group level by a supervisory authority in Gibraltar or in the third country. (Section 23A, POCA).

Weighting and Conclusion

200. Ultimate responsibility of the functions carried out by the third party remains with the RFB. Nevertheless, RFBs are permitted to rely on third parties by simply having “*reasonable grounds to*

¹⁰⁵ Although it is not explicit, this can be interpreted as those countries identified by the European Commission as high risk, since “high risk third countries” is used in other parts of POCA with the respective meaning.

believe” that the third party is regulated and supervised accordingly. Although reliance on third parties established in high risk third countries is not permitted for all other situations there is no requirement to take into consideration information available on the country risk apart from membership to the EEA. Regarding the timing, information and documentation must be made available by the third party “*as soon as reasonably practicable*” rather than immediately and without delay. **R.17 is rated LC.**

Recommendation 18 – Internal controls and foreign branches and subsidiaries

201. Gibraltar was rated LC for the former R.15 and C for R.22 in the 2007 IMF Report. Identified deficiencies included the need to extend consideration of FT issues to controls and training and need to ensure that all licensees have an internal audit program in place.

202. **Criterion 18.1 –**

a) RFBs are required to establish and maintain appropriate and risk-sensitive policies, controls and procedures, proportionate to their nature and size, relating, among others, to compliance management. This includes, *where appropriate* (rather than always) regarding the size and nature of the business, the allocation of overall responsibility for the establishment and maintenance of effective systems of control to a compliance officer at management level (being a director or senior manager) (Section 26(1), POCA). Also, RFBs should, *where applicable* (rather than always), appoint a director, senior manager or partner, and it shall be that person’s duty to ensure compliance with requirements of the Act (Section 9B, POCA).

b) RFBs, having regard to the risks, the nature of the business and its size, must establish and maintain appropriate and risk-sensitive policies, controls and procedures, proportionate to its nature and size, relating to employee screening and must conduct regular training for its employees in ML/FT legislation and monitoring (Sections 26(1) and 27(1), POCA).

c) RFBs should *where appropriate* (as opposed to always) having regard to the size and nature of the business, undertake an independent audit function for the purposes of testing the policies, controls and procedures referred to in subsection (1) (Section 26(1A), POCA). The requirement is reiterated in section 5.5 of the AMLGN that states that the GFSC expects all FIs to conduct an independent audit. FIs have a duty to appoint a Compliance Officer (in a managerial position), where applicable/appropriate (Sections 9B, 26(1)(f) and (1A), POCA). Senior management of firms must ensure the allocation to a director or senior manager the overall responsibility for the establishment and maintenance of effective AML and CFT systems of control and, in addition, the appointment of a person with adequate seniority and experience (MLRO) (R2, AMLGN).

203. **Criterion 18.2 –** There is no direct provision in POCA that requirements regarding employee screening, compliance management arrangements or independent audit function, should be applied group wide. Nevertheless, there is a general requirement for FIs to apply to branches located in third countries the same level of requirements as in Gibraltar, to the extent that the third country’s law so allows (Section 26(5A), POCA). In addition, there are special requirements that cover the provisions of C.18.2 regarding groups and branches, which apply regardless of the location of the branch:

a) RFBs that have branches or subsidiaries must implement group wide policies for sharing information within the group to the extent permitted by GDPR. Any such information shared can only be used for the general purpose of AML/CFT, which includes CDD and ML/TF risk management, although this is not explicitly mentioned as in C.18.2(a) (Sections 26(1B) and (1C), POCA).

b) A group must have in place internal reporting procedures for the purpose of receiving disclosures about knowledge or suspicions of ML/FT. This includes appointing a ML reporting officer (MLRO). Information received under those provisions may be shared inside the group (but is not compulsory) unless instructed otherwise by the FIU (Section 28(1), (2) and (3), POCA). A general provision for sharing information for the purpose of AML/CFT, which could include, but does not explicitly mention, customer, account and transaction, is covered by Sections 26(1B) and 26(1C), POCA.

c) Any sharing of information within the group must take place to the extent permitted by EU General Data Protection Regulation (GDPR), thus applying GDPR provisions as safeguards for confidentiality. Regarding tipping-off, there is a general provision that the disclosure of certain matters relating to AML/CFT constitutes an offence.

204. **Criterion 18.3** – There is a general provision that FIs shall ensure that the level of requirements expected in Gibraltar is applied to branches or majority owned subsidiaries located in third countries, to the extent that the third country’s law so allows (Section 26(5A), POCA). In case of EEA states and territories, there is a general assumption that those have AML/CFT measures consistent with 4th AMLD. Apart from the general provision, CIs and FIs must specifically require their branches and subsidiary undertakings which are in a non-EEA state or territory to apply, to the extent permitted by the law of that state or territory, measures at least equivalent to those of Gibraltar regarding: i) CDD; ii) on-going monitoring; and iii) record-keeping (Section 21(1), POCA; R12, AMLGN). Where the host non-EEA country or territory does not permit proper implementation of those specific AML/CFT measures, FIs should inform GFSC and take additional mitigating measures. The GFSC may require the termination of business in the third country if the firm does not adhere to this obligation (Sections 21 (2) and (2A), POCA). Although the AMLGN mentions that that firms need to consider that some of the more recent members of the EU may have not given effective transposition to the 4th AMLD and may have merely given legislative effect to its requirements (therefore, firms will also need to consider the FATF and IMF reports on each country - section 6.2.4.1.1, AMLGN) there is a presumption in legislation that all EEA countries have similar AML/CFT requirements.

Weighting and Conclusion

205. Some requirements of C.18.1 are only applied by FIs ‘where appropriate’ rather than always. In addition, they do not extend to group level as required by C18.2. Requirements relating to foreign branches and subsidiaries are largely covered by POCA and AMLGN, but they only apply in case of non EEA states and territories, as there is a presumption in legislation that all EEA countries have similar AML/CFT requirements. FIs are required to inform GFSC and take additional mitigating measures when it cannot apply same standard as in Gibraltar, but this is restricted only to standards relating to CDD, on-going monitoring and record keeping, and not to all AML/CFT measures. **R.18 is rated LC.**

Recommendation 19 – Higher-risk countries

206. Gibraltar was rated LC for former R.21 in the 2007 IMF Report. Some deficiencies were identified in relation to the currency exchange offices, stand-alone money transmitters and FT provisions.

207. **Criterion 19.1** – RFBs must apply EDD measures to appropriately manage and mitigate risks when dealing with natural persons or legal entities from third countries identified by the European Commission (EC) as having a high risk (Section 17(1), POCA) Additionally, RFBs are required to examine the background and purpose of all complex or unusual transactions that have

no economic or lawful purpose. The RFB must increase its monitoring of the business relationship in line with these concerns (Section 17(3), POCA). The EC has identified these countries in Commission Delegated Regulation (EU) 2016/1675, which acknowledges the categorisation done by the FATF and is closely aligned to the statements issued by the FATF. Section 24 of the POCA grants the Minister with authority to take certain steps and actions in regard to a person who is situated in a non-EEA state or territory when called for by the FATF. R57 of the AMLGN states that firms must take additional measures with transactions of business relationships whose source of funds derives from NCCT or sanctioned countries and territories (identified by FATF).

208. **Criterion 19.2** – For customers situated or incorporated in non-EEA states or Territories for which the FATF has decided to apply countermeasures, the Minister may instruct a RFB not to enter into, to terminate a business relationship or not to carry on an occasional transaction (Section 24(1), POCA). Independently of any call from the FATF, in cases of high risks identified by the RFB or by the Minister, RFBs must apply EDD to appropriately manage and mitigate the risks (Section 17(1), POCA). The Minister can impose further action, by notice in the Gazette, in other cases of higher risk identified (Section 17(1)(c)(ii), POCA).

209. In cases of branches situated in non-EEA countries or territories that do not permit the application of equivalent AML/CFT measures, the GFSC exercises additional supervisory actions, including requiring that the group does not establish or that it terminates business relationships, and does not undertake transactions and, where necessary, requesting the group to close down its operations in the third country (Section 21 (2A) of POCA).

210. **Criterion 19.3** – The GFSC publishes information on its website provided by the FATF on countries which present a higher ML/FT risk for reference to all licensees. This is published as and when the FATF issues its press releases and/or notices and licensees are advised when this is issued on the GFSC website. There is on-going external engagement between the GFSC and all regulated entities with regards to the ML/FT risks, as necessary.

Weighting and Conclusion

211. Gibraltar has mechanisms in place regarding higher-risk countries when called upon by FATF or independently. Nevertheless, some provisions (Criterion 19.2) apply only to non-EEA countries and territories. **R.19 is rated LC.**

Recommendation 20 – Reporting of suspicious transaction

212. In the 2007 IMF assessment report Gibraltar was rated LC with former R.13, as there was some confusion over to whom to report; and STRs on attempted transactions were not explicitly required.

213. **Criterion 20.1** – Section 4G of the 2015 POCA, stipulates that a disclosure is authorised to the GFIU, a police officer, a customs officer or a nominated officer, if the property is criminal property. In addition, S.4G(3C) stipulates that the disclosure is made on his own initiative and as soon as is practicable after he first knows or suspects that the property constitutes or represents a person's benefit from criminal conduct. S.182(1A) defines criminal property as (a) a person's benefit from criminal conduct or it represents such a benefit (in whole or part and whether directly or indirectly); and (b) the alleged offender knows or suspects that it constitutes or represents such a benefit.

214. As regards FT reporting, section 40 - 47 of the 2018 Terrorism Act provides for the reporting of suspicion or belief that money or other property is terrorist property. If a person suspects or has reasonable grounds to suspect that a person is engaged in FT, it is an offence not

to disclose as soon as is reasonably practicable (S.40 (3) of the Terrorism Act 2018). Assessors were satisfied that the 'as soon as is practicable or reasonably practicable' threshold meets the requirement for SARs to be reported promptly once a suspicion is formed.

215. **Criterion 20.2** – POCA S.6B(1) refers to the obligation of a person to report all suspicious transactions, including attempted transactions, regardless of the amount of the transaction. There are no minimum thresholds for reporting under the POCA.

Weighting and Conclusion

216. All criteria are met. **R.20 is rated C.**

Recommendation 21 – Tipping-off and confidentiality

217. In the 2007 IMF assessment report Gibraltar was rated C with former R.14.

218. **Criterion 21.1** – The POCA (section 4H) and the Terrorist Act (section 10) provides a broad protection to persons who make a disclosure to the GFIU, a police officer, a customs officer or a nominated officer in good faith. This protection is available for any authorised disclosure made in good faith, even if the person making the disclosure did not know or suspect that the property constituted or represented a person's benefit from criminal conduct, the act was not a prohibited act (POCA s.4G(3(b)) and s.4G(6)).

219. **Criterion 21.2** – The POCA (section 5) provides that a person is guilty of an offence if he discloses the fact that a STR or related is filed with the GFIU.

Weighting and Conclusion

220. All criteria are met. **R.21 is rated C.**

Recommendation 22 – DNFBPs: Customer due diligence

221. Gibraltar was rated PC for the former R.12 in its 2007 IMF Report. While there were numerous deficiencies in the requirements for DNFBPs on CDD, PEPs, etc., two key areas of risk (TCSPs and internet-based gambling) were subject to more robust standards through the AMLGNs. Since then, Gibraltar has extended the statutory AML/CFT requirements to the DNFBPs. Requirements for DNFBPs are now primarily set out in the POCA. In addition, DNFBPs must comply with the guidelines issued by each respective regulator or supervisors. There should be no conflict between any advice issued in guidelines and the law. However, if there is, then the law prevails.

222. For gambling providers further provisions are set in 2 sectoral Codes of Practice, the General Gambling Guidelines (2016) and the Remote Gambling Guidelines (2018). For HVDs and REAs two separate but similar guidance has been issued. No sectoral guidance has been issued for accountants and tax advisors, while insolvency practitioners are covered by the AMLGN. TCSPs are also covered by the AMLGN. Lawyers, notaries and other independent legal professionals are covered, apart from the POCA, by guidance issued by the RSC.

223. In the analysis presented below, the deficiencies identified in relation to the compliance of FIs with the FATF requirements under respective Recommendations are also relevant, where applicable, for the DNFBPs, unless specified otherwise.

224. **Criterion 22.1** – POCA applies to FIs and DNFBPs equally, as DNFBPs are listed as RFBs under POCA (Section 9(1)). For TCSPs AMLGN apply (providing some additional requirements to POCA as described under R.10), while for the other DNFBPs, not all shortcomings in POCA are

covered with sectoral Guidelines. In addition, the following deficiencies have been identified: in case of casinos and legal professions, exemption from CDD requirements are provided by guidelines, not based on a proven low risk; RSC Guidance provides that a legal professional is not required to obtain information on the nature and purpose of the business relationship or on BOs and on-going monitoring is not required, if SDD is applied (Section 4.8.1, RSC Guidance).

225. **Criterion 22.2** – POCA applies to FIs and DNFBPs equally, as DNFBPs are listed as RFBs under POCA (Section 9(1)). The deficiencies identified under R.11, mainly not requiring record keeping for all CDD information are in part covered by some of the sectoral Guidelines. For example, HVDs/REAs are explicitly required to record and store for 5 years CDD documents and information. This includes account files and business correspondence where relevant (Section 7, HVD Guidelines; Section 7, REA Guidelines). Guidance notes for legal profession require record-keeping for CDD material. However, they do not include explicit requirement to gather records in the way that they would enable the reconstruct of the transactions. There is also no requirement that records must be made available swiftly to competent authorities (Section 3.8.1, RSC Guidance). Nevertheless, as noted in R.11, the principle for CDD record-keeping should be mentioned in law.

226. **Criterion 22.3** – The provisions of the POCA that cover PEPs apply to DNFBPs accordingly, as they are listed as RFBs under POCA (Section 9(1)). In addition to deficiencies noted under R.12 following shortcoming has been identified: PEPs are identified on a risk sensitive basis by casinos as the authorities do not expect every customer to be ‘PEP checked’ (3.26-3.27, General Gambling Guidelines; 8.1 and 8.2, Remote Gambling Guidelines).

227. **Criterion 22.4** – The provisions of the POCA that cover new technologies apply to DNFBPs accordingly, as they are listed as RFBs under the POCA (Section 9(1)). Requirement in AMLGN to undergo ML/TF assessment prior to the launch of a new product only applies only to TCSPs and not to other DNFBPs. Remote gambling providers are only required to consider the development of new products and business practices as well as the use of new or developing technologies, including giving due attention to the ML/FT risks that may arise before their launch (5.6, Remote Gambling Guidelines). RSC Guidance do not provide explicit requirements regarding new technologies, due to the specificity of the legal profession. Nonetheless, lawyers and notaries are required to always remain vigilant to the evolving nature of cybercrime and the dangers of identity theft, in relation to electronic verification of identity (Section 4.3.3.3 of the RSC Guidance). DPMSs are covered by FATF Recommendations only when they engage in cash transactions while REAs do not participate in the actual financial transactions. This, combined with the distinctive activity *per se*, limits the possibility for developing new products, technologies or practices as referred to in R.15.

228. **Criterion 22.5** – The provisions of POCA that cover reliance on third parties apply to DNFBPs accordingly, as they are listed as RFBs under the POCA (Section 9(1)), therefore the deficiencies identified under R.17 apply. There are no specific provisions in the sectoral guidelines to address these deficiencies.

Weighting and Conclusion

229. Some deficiencies identified in R.10, 11, 12, 15 and 17, based on provisions of POCA have been covered by sectoral guidelines, such as record keeping for HVDs, REAs and legal professions. However, other new deficiencies arise. **R. 22 is rated PC.**

Recommendation 23 – DNFBPs: Other measures

230. Gibraltar was rated PC for former R.16 in the 2017 IMF Report. Reporting requirements and tipping off provisions were appropriately in place, but significant attention was needed on requirements for audit and dealing with clients from outside of Gibraltar. In addition, the former lack of effective oversight of most DNFBPs other than the GFSC supervised TCSP sector, created an inability to assess the effectiveness of the provisions that were in place and lack of an appropriate range of sanctioning powers limited the ability to ensure corrective action.

231. Requirements for DNFBPs, are primarily set out in POCA, as they are listed as RFBs. Aside from POCA, DNFBPs must apply sector specific guidance issued by each respective regulator/supervisor. There should be no conflict between any advice issued in guidelines and the law. However, if there is, the law prevails.

232. In the analysis presented below, the deficiencies identified in relation to the compliance of FIs with the FATF requirements under respective Recommendations are also relevant, where applicable, for the DNFBPs, unless specified otherwise.

233. **Criterion 23.1** – The provisions of the POCA cover DNFBPs accordingly, as they are listed as RFBs under the POCA (Section 9(1)). Thus, the R.20 analysis applies.

234. **Criterion 23.2** – The provisions of the POCA that cover internal controls and foreign branches and subsidiaries apply to DNFBPs accordingly, as they are listed as RFBs under the POCA (Section 9(1)). Therefore, the analysis and deficiencies identified under R.18 apply. Also, for some provisions, materiality was considered, for example there is only one land-based casino in Gibraltar, and it has no branches.

235. **Criterion 23.3** – The provisions of the POCA that cover higher-risk countries apply to DNFBPs accordingly, as they are listed as RFBs under the POCA (Section 9(1)). Thus, the analysis and deficiencies identified under R.19 apply.

236. **Criterion 23.4** – The provisions of the POCA that cover tipping-off and confidentiality apply to DNFBPs accordingly, as they are listed as RFBs under the POCA (Section 9(1)). Thus, the analysis under R.21 applies.

Weighting and Conclusion

237. Based on deficiencies identified in R.18 and 19 which are equally relevant to DNFBPs, **R. 23 is rated LC.**

Recommendation 24 – Transparency and beneficial ownership of legal persons

238. Gibraltar was rated LC for R.33 in the 2007 IMF report. The report noted that bearer share to warrants should be abolished and that the Companies House registry should be searchable by multiple fields. Since then, the FATF standard has changed substantially.

239. **Criterion 24.1** – For the purpose of R.24 the following types of legal persons are relevant for the analysis: public and private companies with limited and unlimited companies, private foundations, protected cell companies, Limited Liability Partnerships (LLPs), European Economic Interest Groupings and European companies.

240. Gibraltar has mechanisms that identifies and describes the different types, forms and basic features of legal persons. Public and private companies limited and unlimited companies are described in the Companies Act (CompA), sectoral laws (private trust companies, private foundations, and protected cell companies) as well as online on the website of the Companies

House Registry (CHG)¹⁰⁶ (European Economic Interest Groupings (EEIGs)¹⁰⁷, Public limited companies, European companies, LLPs, protected cell companies, private trust companies and private foundations). These mechanisms describe also the processes for the creation of the legal persons. Information on the basic ownership is regulated by the CHG Guidance Note numbers 5, 7 and 8 (on searches, certificates of good standing, and profiles respectively). Information for obtaining and recording BO information is in the 2017 Regulations on the Register of Ultimate Beneficial Owners (RUBOR).

241. **Criterion 24.2** – Both the 2016 and 2018 NRA consider the risks of ML/FT associated with all types of legal persons created in country. However, while the assessment looks at general vulnerabilities (such as nominee shareholdings and creation of complex and opaque structures) and at the general types of activities (noting that Gibraltar legal entities are commonly used both as asset holding, investment and transactions based vehicles for both the domestic as well international community), it is not very specific, as it does not analyse the inherent vulnerabilities of the specific types of legal persons that can be created in Gibraltar or their activities.

242. **Criterion 24.3** – All companies created in Gibraltar are subject to mandatory registration with the CHG. The information held on the public record of the companies registered with CHG includes the company name, proof of incorporation (i.e. the incorporation certificate issued in accordance with section 15 of the CompA), legal form and status, the address of the registered office address, the Memorandum of Association (Section 9, CompA); Articles of Association (Section 22, CompA) and particulars of directors or managers, and secretaries. This information is publicly available, upon request and payment of a fee, except for the foundation charter for overseas foundations (foundations established abroad that re-domicile and register in Gibraltar), where this information is not publicly available. A company can be engaged to act as director or shareholder of a Gibraltar company. In the case of a foundation the councillor of the foundation may be a corporate. A foundation registered under the Private Foundation Act (PFA) must have a Gibraltar resident body corporate holding a Class VII license (i.e., a licence issued under section 8 of the Financial Services (Investment and Fiduciary Services) Act and classified as a Class VII licence under Schedule 1 to the Financial Services (Licensing) Regulations 1991) on its Foundation Council (section 24.(1), PFA).

243. **Criterion 24.4** – Companies that are subject to the CompA are required to maintain at their registered office: i) a list of directors and managers (S 222 of the CompA); ii) a register of members (or shareholders). The list of directors and members must be kept at the registered office of the company, which, according to the law, must be in Gibraltar. The registered office address must be notified to the CHG as part of the application to register the company. If the company has a share capital, the prescribed particulars of the rights attached to the shares of each class is one of the criteria that must be included in the statement of capital and initial shareholdings required to be filed with the CHG in the case of a company that is to have a share capital (Section 10, CompA). In this case the register of member also requires to note a statement of the shares held by each member, distinguishing each share by its number and of the amount paid or agreed to be considered as paid on the shares of each member (Section 182, CompA). Foundations are required to keep a registered office in Gibraltar and maintain a list of councillors. As regards LLPs, the provisions of Section 182 of the CompA in respect of the requirement to keep a register of members extends to LLPs by virtue of regulation 6 of the LLPs (Application of Companies Act 2014 and Insolvency Act 2011) Regulations 2016. On incorporation, the members are the persons who subscribed their names to the incorporation document (Section 6(1), LLPA).

¹⁰⁶ <https://www.companieshouse.gi/index.html>

¹⁰⁷ <https://www.companieshouse.gi/publications/C0011.pdf>

244. **Criterion 24.5** – When making decision on registration of the legal person reviews the application and provided documents for their completeness the CHG must be satisfied that the documents submitted, and the information provided for registration meet the requirements set out in the relevant law. All registered companies, LLPs and foundations are obliged to make annual returns to the CHG, and to file with the same when there is a relevant change that must be notified to the CHG (Section 426, Companies Act). This includes changes in membership/shareholders, address of the registered company and directors, *inter alia*. However, the sanctions for late filing of changes of the basic information are very low (only 17,50 GBP, Section 426 (4) (c), Companies Act).

245. **Criterion 24.6** – Gibraltar utilises various mechanisms to ensure access to information on the BO of a legal person:

a) corporates and legal entities (LEs) incorporated in Gibraltar are required to obtain and hold adequate, accurate and current information on the BO of the corporate or LE, including the details of the beneficial interests held (Regulation 6, RUBOR). A foundation is also required, by virtue of Regulation 11A of the RUBOR, to obtain and hold adequate, accurate and current information on the BO.

b) Gibraltar has created the RUBO, a register with information on BOs of all entities incorporated in Gibraltar. Regulation 8 of RUBOR requires for all LEs incorporated in Gibraltar to submit information on the ultimate BOs of the corporate or LE or of any change within 30 days of incorporation or within 30 days beginning with the date of the occurrence of the change. This requirement applies also to corporate and LEs which were in existence prior to the enactment of the RUBOR. However, the form for the submission of information to the RUBO contemplates also the option to consider a “relevant legal entity” as an ultimate BO (Part B.4), which is not in line with the FATF definition of BO, which refers to a natural person. In addition, there are no sanctions for non-compliance with the requirement to provide the information within 30 days of the change (for corporate or LEs incorporated prior to the commencement of the RUBOR) or with the requirement to provide the information within 30 days of its incorporation (for corporate or LEs incorporated after the commencement of the RUBOR)¹⁰⁸.

c) FIs and TCSP, as entities subject to the POCA are required to identify and take risk-based measures in verifying the BOs of an entity and authorities have access to this information. However, the deficiencies identified under R.11 on the record keeping requirement for the BO affect the consistency of this criterion.

246. **Criterion 24.7** – Corporates and LEs incorporated in Gibraltar are required to obtain and hold adequate, accurate and current information on the BO of the corporate or legal entity, including the details of the beneficial interests held (Regulation 6, RUBOR). This is subject to a criminal sanction. They are also required to notify the Registrar of any relevant change. In addition, the RUBOR requires that a person who is an ultimate BO of a corporate or legal entity incorporated in Gibraltar to inform the corporate or LEs of their status as an ultimate BO (Regulations 8A, RUBOR); however, there is no sanction for non-compliance with this requirement. These shortcomings, together with the ones noted under C.26 b) and c) affect the accuracy and relevance of the BO information.

247. **Criterion 24.8**

a) There is no requirement to have a specific contact accountable to competent authorities in notifying of the relevant BO information, instead, all members of a company’s senior management are responsible for the company’s obligations, and therefore, they are all obliged to ensure that the company complies with its legal obligations of registering the BO data, etc.

¹⁰⁸ See Regulations 42.1

b) There is no specific provision requiring that a DNFBP be authorized by the company and accountable to competent authorities for providing all basic and available BO information. For those LEs that are managed by a TCSP or subject to auditing requirements, the requirements for TCSP and auditors to identify and verify the client and to identify and take risk-based measures to verify the identity of the BO; to keep this information and provide it to the authorities would apply.

248. **Criterion 24.9** – There are no specific requirements for persons involved in the dissolution of a company to maintain and records referred to in this criterion, but only a requirement to maintain records and information related to the insolvency of the company and the insolvency work,¹⁰⁹ for a period of at least 6 years after the liquidator’s appointment has ceased to have effect. As regards the Registrar, Regulation 25 of the RUBOR requires that Registrar maintain records of all information received indefinitely. For those LEs that are managed by a TCSP or subject to auditing requirements the record keeping requirements for these professionals under POCA apply (Section 25 of POCA requires firms to maintain records for at least 5 years following completion of a transaction and the end of a business relationship).

249. **Criterion 24.10** – As regards information in the RUBO, this can be accessed and obtained by the FIU and any other “*competent authority*”. Where the LEAs require BO data, other than already available from the RUBO, and it is investigating a crime and the company is serviced by a TCSP, a CP&EA Schedule 1 Production Order can be used to obtain the data. The same investigative method can be used to obtain BO data contained in the CDD held by a FI. In relation to the company itself, a search warrant can be obtained in a criminal investigation to search the company’s premises whereby data relating to UBO’s can be seized. Powers of search are explained in R.30. The GFSC has also access to basic and BO information maintained by the entities subject to POCA and to CDD-related requirements.

250. **Criterion 24.11**– Bearer shares cannot be issued by Gibraltar registered companies. A person who agrees to become a member, becomes a member of a company upon that person’s name being entered in the company’s register of members. It is not possible to issue shares to an unnamed person. Until 2013 it was possible to issue bearer share warrants, but the CompA was amended, so that no rights attached to a share warrant issued prior to 21 March 2013 can be exercised unless the bearer has been entered in the company’s register of members (Section 157(3), CompA). According to the authorities, there is no active company registered in Gibraltar with shares issued to bearer or with share warrants issued to bearer.

251. **Criterion 24.12** – There is no prohibition against nominee shareholders and directors. Persons providing nominee services (including acting as or providing nominee shareholders) on a professional basis are required to be licensed by the GFSC under the FS(IFS)A, and subject to POCA (including identifying the BO, if it is the nominator, and keep records). Nominee shareholders that are not acting by way of business are not regulated. There is no requirement for licensed nominee shareholders or directors (or for nominee shareholders or directors in general, and for non-licensed nominee directors or shareholders to maintain information identifying their nominator. As discussed earlier there are requirements to notify the CHG about directors, but there is no requirement for nominee shareholders and directors to disclose the identity of the nominator to the company or to the register maintained by the CHG.

¹⁰⁹ Regulation 16. (1) of the Insolvency Practitioner Regulations 2014 requires an insolvency practitioner to (a) maintain in respect of his insolvency practice–
(i) records and details of each appointment as receiver, administrative receiver, administrator, interim supervisor, supervisor, provisional liquidator, liquidator, voluntary liquidator or bankruptcy trustee; and
(ii) case records, working papers and all proper documents relating to all insolvency work undertaken.

252. **Criterion 24.13** – The CompA provides sanctions for non-compliance with the information filing requirements, but only in the case of late submissions. In this case fees can be levied, which are not dissuasive nor proportionate, as they are only between 17,50 GBP (which applies to most of the filings, e.g. change of registered office, directors, shareholders) and 117 GBP (for the late filing of accounts, but only after 2 years of not providing them) and 141,50GBP (for the late lodging of the annual return, but only after the third year) in the case of not filing changes of information. For the lack of submission, the Registrar has only a faculty to strike off the register the name of any company, other than a public limited company, in respect of which no annual return has been filed in the previous 3 calendar years. With respect to the record keeping and registration of BO information, RUBOR has provision for civil penalties and criminal penalties. However there are no sanctions for non-compliance with the requirement to provide the information within 30 days of the change (for corporate or LEs incorporated prior to the commencement of the RUBOR) or with the requirement to provide the information within 30 days of its incorporation (for corporate or LEs incorporated after the commencement of the RUBOR). Section 42 of RUBOR provides for civil penalties by the Register to impose a penalty of such amount as he considers appropriate for non-compliance with the Regulations. Whilst Section 45 of RUBOR provides for criminal penalties of a fine or imprisonment.

253. **Criterion 24.14** – Gibraltar ensures international cooperation in relation to basic and BO information through various channels:

a) Basic information maintained by the CHG is available publicly and/or may be requested and obtained by any person, including foreign competent authorities. As regards documents, they can only be provided by the Registrar, if the Registrar thinks it fit, as provisioned for in Section 427 of the CompA.

b) Section 26 of the RUBOR permits competent authorities to request information relating to an express trust, a corporate or a legal entity incorporated in Gibraltar, which include information on the beneficial owner, albeit with the limitation noted in the analysis of C.24.6. The GFSC can obtain information with respect to any regulated entity, or its customers, under Section 6 of the FS(IG&C)A. This information may then be disclosed to the authority of another jurisdiction, as per Section 4(3) of the FS(IG&C)A. Law Enforcement Agencies can exchange information through a variety of channels, including MLA and police-to-police assistance.

c) However, the issues noted in regard to the lack of sanctions in regard to the RUBO, the issue noted in regard to record keeping requirements for the BO, which may affect the accuracy and relevance of the information that can be obtained, could have a negative impact on the rapidity required by this criterion for the exchange of the information.

254. **Criterion 24.15** – Various mechanisms exist for the request of information from other jurisdictions. Formal networks such Egmont are processed through FIU. GCID receive and make formal requests via Interpol's system. The RGP conducts external enquiries with Schengen contact points, especially with LEAs in Spain. The RGP are also members of the informal international networking groups CARIN and AMON. Gibraltar has not sought BO data internationally and therefore this has not arisen.

Weighting and Conclusion

255. Gibraltar has taken a number of measures to prevent the misuse of legal persons for ML or TF. However, no comprehensive risk assessment of the ML/FT risk associated with all types of legal persons; no requirement for licensed nominee shareholders or directors to maintain information identifying their nominator and to disclose the identity of the nominator to the company or to the register maintained by the CHG. Sanctions for non-compliance with the filing of

information with CHG exist only in the case of late submissions and are not proportionate nor dissuasive. Although Gibraltar has in place a number of mechanisms to access BO information, the shortcoming noted in the analysis, including those related to R.11, may affect the completeness and accuracy of the information and timeliness of access. **R.24 is rated PC.**

Recommendation 25 – Transparency and beneficial ownership of legal arrangements

256. Gibraltar was rated LC for R. 34 in 2007 IMF report. The report noted the continued existence of asset protection trusts and flee clauses, and that competent law enforcement authorities may not have access in a timely fashion to adequate, accurate and current information on beneficial ownership and control. As the requirements in R.25 have changed considerably since then, the 2007 IMF report analysis is no longer relevant. Gibraltar has several different types of trusts that are regulated or governed under various Gibraltar’s law: the Asset Protection Trusts¹¹⁰ (ATP – Bankruptcy Law); the Private Trust Company¹¹¹ (PTC – Private Trust Company Act), discussed under R.24 but also relevant under R.25 as the company acts as a trustee; purpose trusts (PT – Purpose Trust Act), which can be established for non-charitable purposes (e.g. asset holding vehicles). The Trusts (Private International Law) Act of 2015, is a firewall legislation to protect trusts established in Gibraltar from foreign laws or judgments. Gibraltar legislation does not still proscribe the inclusion of “*flee clauses*” in the trust instrument. Therefore, trusts in Gibraltar may include such clauses. The occurrence of an event triggering the “*flee*” would be typically set in the trust deed, but it can be in a way that leaves broad discretion to the trustee to determine such occurrence and entitle him/her to move the assets of the trust elsewhere.

257. Criterion 25.1 –

a) (Partly Met) – The following legal provisions address this requirement:

Regulation 9 of the RUBOR requires a trustee of an express trust to obtain and hold adequate, accurate, and up-to-date, information on the BO of the express trust, which, as per the definition of BO of the RUBOR, includes the settlor, the trustee, the protector and beneficiaries or class of beneficiaries. This requirement applies also to any other legal arrangements similar to trusts (Regulation 11A, RUBOR). However, this requirement does not apply to express trusts “*governed under their law*”, as per the FATF definition, but only to a trust (or similar legal arrangement) that “*generates tax consequences in Gibraltar*”. Given that the assets held by many trusts created in Gibraltar may be held abroad, this limits further the amount of BO information on trust that can be available in the RUBO.

Gibraltar has also a general law on Trustees (the Trustees Act) which has a provision (S 61) requiring trustees to record in writing the information on the identity of the settlor, trustee,

¹¹⁰ APTs are registered with the FSC under the Bankruptcy (Register of Dispositions) Regulations. Information on the country and ordinary residence of the Settlor are included as part of the registration process. The identity of the settlor is not submitted to the FSC. However, the trustees will be Professional Trustees subject to the full requirements of POCA which includes CDD on the settlor. The identity of the settlor would therefore be available to the FSC.

¹¹¹ The private trust company’s sole purpose is to act as trustee to the trust (or group of trusts) belonging to the group. It is usually formed to act as trustee for specific individuals or groups of individuals and entities where the parties are all related to some extent. The PTC trustee may not be compensated for its services unless it is licenced by the FSC. A PTC in Gibraltar has to be administered by a licenced and regulated company manager or trustee in Gibraltar. Whilst they are subject to the normal regulatory regime and must exercise the duties and powers of a trustee in the usual way, these can be less restrictive because they look after the interests of only one or a few families

beneficiaries, class of beneficiaries, protector and any natural person exercising control over the trust, although no requirement that this information be adequate, accurate and current.

Regulation 12 of the RUBOR requires a corporate or LE or an express trust to take reasonable steps-(a) to find out if there is anyone who is a BO in relation to the express trust, corporate or legal entity and (b) if so, to identify them. However, pursuant to sub regulation 12.1 only a corporate or legal entity incorporated in Gibraltar must keep records of the actions taken in order to identify the BOs. This requirement does not apply to trusts, but only to a corporate or LE.

Professional trustees are subject to POCA, and they are required to identify and take reasonable measures to verify, on a risk sensitive basis the identity of the BO, which, in the case of trusts includes the settlor, the trustee, the protector and the beneficiary (or class of beneficiary). However, a PTC that acts as a trustee is not licensed by the GFSC and not subject to CDD requirements (only their registered administrators are). In this case S 61 of the Trustees Act applies as the general rule noted above. The record keeping requirements stipulated by POCA apply only to customer's information, and not explicitly BO's. It is unclear what is the relation between the requirements stipulated by RUBOR and by POCA if a professional trustee is also a trustee of an express trust.

b) (Partly Met) – There is no requirement for trustees of any trust governed under their law to hold basic information on other regulated agents of, and service providers to, the trust, including investment advisors or managers, accountants, and tax advisors. The GFSC AML Guidance (R86) provides only that *“firms should take adequate measures in ascertaining whether the trustees of the trust hold basic information on other regulated agents of, and service providers to, the trust. This can include, but is not limited to, investment managers or advisors, accountants and tax advisors”*, which is not the same.

c) (Partly Met) – Applicable with the limitations noted under 25.1(a). Professional trustees are subject to the record keeping requirements established by POCA (S. 25) However, these requirements apply only to customer's information, and not explicitly BOs.

258. **Criterion 25.2** – Professional trustees are subject to CDD and record keeping requirements, and, as noted in the analysis of 25.1 trustees of an express trust must obtain and hold adequate accurate and up-to-date information. See the shortcomings noted under C. 25.1

259. **Criterion 25.3** – No requirement for trustees to disclose their status to FIs and DNFBPs.

260. **Criterion 25.4** – Pursuant to Regulation 11 of RUBOR, trustees are required to submit information on the trust to the RUBO. Section 61A of the Trustees Act requires trustees to comply with a request for information under regulation 41A of the RUBOR within 10 working days of receipt of such request (this provision applies also to trustees of an express trust that does not generate tax consequences in Gibraltar) Professional trustees licensed by the GFSC are also subject to the powers to request information stipulated by the SBPR and the FS(IG&C)A. There are no provisions that prevent the trustee from providing FIs and DNFBPs, upon request, with information on BO and the assets of the trust to be held or managed under the terms of the business relationship.

261. **Criterion 25.5** – professional trustees are defined as a RFBs under Section 9 of POCA, the full range of investigative powers are available to the law enforcement and investigative authorities as well including the enforcement powers afforded to competent authorities as stated within the SBPR.

262. **Criterion 25.6** – Gibraltar's legal framework allows authorities to provide international co-operation relating to information on trusts and other legal arrangements. Law enforcement authorities can exercise domestically available investigative powers to obtain information from

trusts, including beneficial ownership information, on behalf of non-Gibraltar authorities through MLA or (including for non-law enforcement authorities) direct agency-to-agency assistance. The GFSC can assist other competent authorities whether these are foreign or not, in the exchange of information, under the provision of Section 12 of the FS(IG&C)A. The legislation does not differentiate between the provision of BO data separately, so this is encompassed generally. BO data can be obtained through the FIU: under the provisions of the POCA (Sec 1J(1)), the FIU is able to exchange intelligence with domestic law enforcement and supervisory bodies list in Schedule 2, Part 1 of POCA. The issues noted in regard to the lack of sanctions of certain requirements of the RUBOR, as well as the deficiencies identified regarding the record keeping requirements (R.11) may affect the accuracy and relevance of the information that can be obtained and could have a negative impact on the rapidity required by this criterion for the exchange of the information.

263. **Criterion 25.7**– Professional trustees are subject to the sanctions established by POCA and to the sanctions that can be imposed by the GFSC and to the criminal sanction provided sanctions provided by Regulations 42 and 45 of the RUBOR, which provide for civil and criminal sanctions, respectively. The civil sanction is capped at GBP 10.000 euros, which is not dissuasive. However, there are no sanctions in the case of non-professional trustees and in the case of non-compliance with the requirement to provide the information within 30 days of the change (for trusts created prior to the commencement of the RUBOR) or with the requirement to provide the information within 30 days of its incorporation (for trusts after the commencement of the RUBOR).

264. **Criterion 25.8** – There is a range of civil and criminal sanctions available to grant authorities timely access to information regarding the trust. These sanctions are dissuasive and proportionate, save for the civil penalty established by Regulation 42 of RUBOR noted under C.25.7. Professional trustees are also subject to the criminal sanctions pursuant to Regulation 16 of the FS(IG&C)A (Regulation 16(1) – it is an offence and liable on conviction on indictment to imprisonment for 2 years and to a fine, if a person refuses to supply information or co-operate with the GFSC, or any other body appointed on behalf of the GFSC; Regulation 16(2) – it is an offence to refuse or fail to provide information or such books or documents requested under the Act. The person is liable on summary conviction to a fine.). Trustees of an express trust are also subject to a fine for not complying with a request of information pursuant to the RUBOR (S63 of the Trustees Act, this is a fine up to level 5 on the standard scale – that is GBP 10,000, which is not proportionate or dissuasive)”.

Weighting and Conclusion

265. Although Gibraltar has in place a number of measures to prevent the misuse of legal arrangements for ML/FT and mechanism to access BO information held by trustees, the limited applicability of RUBO requirements to trust that produce tax consequences and the other shortcoming noted in the analysis, including those cascading from R10 and R11, may affect the completeness and accuracy of the information and timeliness of access to BO information. Sanctions are not available in all instances. No requirement for trustees to disclose their status to FIs and DNFBPs or to hold basic information on other regulated agents of, and service providers **R.25 is rated PC.**

Recommendation 26 – Regulation and supervision of financial institutions

266. Gibraltar was assessed PC for R.23 in the 2007 IMF report. The report noted the absence of supervision for the *bureaux de change* or the non-bank money remitter; no specific standards that prohibit criminals or their associates from holding key ownership or management positions in financial institution.

267. **Criterion 26.1 (Met)** – Schedule 2 of the POCA lists the relevant supervisory bodies and designates the GFSC for these purposes in relation to all FATF-designated FIs.

268. **Criterion 26.2 (Met)** – The GFSC is the appointed supervisory body for the list of Supervisory Acts as defined in GFSC(SA)O, and it is responsible for the Authorisation, Regulation and Enforcement of FIs, which include Core Principle FIs. Although there is no explicit requirement, the prohibition for the establishment or continued operation of shell banks arises through the nature and requirements of Gibraltar’s licensing and regulatory process. In particular Section 23 of the Financial Services (Banking) Act sets out that the GFSC shall not grant an authorisation unless it is satisfied that the applicant will be “(b) carrying on the business (i) in Gibraltar or (ii) in Gibraltar and the other country where head office is located” where its head office is established in another country. Furthermore, the GFSC has a mind and management policy which requires all firms to ensure that the business is conducted from its office in Gibraltar, and that the firm can evidence this.

269. **Criterion 26.3 (Partly Met)** – Section 30C of POCA, only requires that a supervisory authority make inquiries with the Commissioner of Police to evaluate whether:

(a) a person who is or intends to be-

(i) a controller of a RFB;

(ii) a BO of a RFB; or

(iii) a shareholder of a RFB;

(b) a person who holds or intends to hold a senior management position in a RFB; or

(c) an associate of a person under either paragraphs (a) or (b), has a relevant criminal conviction. Therefore, the “legal” measures established by POCA consist in requiring a supervisor to make inquiries to determine whether the subjects mentioned in the provision have a criminal conviction. The requirement for an associate to have a criminal conviction may not fully cover all situations of association to a criminal (there could be credible sources indicating association to a criminal but not a conviction).

270. Other legal measures concerning fit and proper are scattered in sectoral laws, with a not always uniform approach as to whom the requirements apply and their scope. For example the Financial Services (Insurance Companies) Act requires fit and proper for “*Each director, controller, manager or main agent of the insurer*”, whereby the Financial Services (Banking) Act requires them for “*every person who is to be a director, controller, shareholder controller or manager*” and the Financial Services (Investment and Fiduciary Services) Act to “*the applicant or any person associated with the applicant*”, whereas the Financial Services (Capital Requirements Directive IV) Regulations apply them the shareholders or members. As regards the what constitutes fit and proper the approach varies, e.g. in the case of insurer it is not expressly defined; in the case of banks it is defined with reference to probity, commission of certain offences and other factors; in the case of capital requirements firms it is the reputation and whether there are reasonable grounds to suspect that, in connection with the proposed acquisition, ML or TF “*is being or has been committed*”. Except for the investment and fiduciary cases (where the commissioner will have “regard” to) in all other cases the commissioner “*shall not*” grant a licence in case of failure of fit and proper requirements. These requirements do not apply to the BO. Only in the case of investment and fiduciary firms there is a specific provision that fit and proper applies also in the case of any person associated with the applicant.

271. In addition to these measures, the GFSC has set out measures that, albeit with some deficiencies, aim at complying with the requirement of this criterion, which are provided for in the

2016 Policy Statement on the Assessment of Fitness and Propriety and in the Due Diligence Methodology framework. This framework provides guidance for considering ML and TF risks posed by individuals or ownership corporate entities that hold a notifiable or controller position of a licensee¹¹². “Controller Notifiable Applicants” are any controllers that exceed 10% shareholding in an entity as applicable. In terms of scope of application, these measures, as well as the sectoral legal measures referred to above do not extend to beneficial owners of a significant or controlling interest, which is an issue not only in the case of corporates, but also on trusts, since the measures apply only to the trustee (and not to the settlor, protector or beneficiaries). This is a significant shortcoming, considering also that POCA specifically distinguishes the BO from the controller when requiring that a supervisory authority make inquiries with the Commissioner of Police.

272. The Due Diligence Methodology explains that honesty, integrity and reputation imply evaluating whether an individual has been convicted of a crime or been subject to any investigations or adverse findings in civil or in disciplinary proceedings (but not in criminal proceedings, although the questionnaire for the applicants for controller mentions also criminal investigations). In the former, the GFSC will be particularly concerned with offences that involve dishonesty, fraud, financial crime or an offence under legislation relating to ML, consumer protection or specific areas of financial services; in the latter, the GFSC will be particularly concerned with investigations or findings that relate to misconduct, fraud or are connected to financial businesses or with the contravention of regulatory requirements. However, there will only be a presumption that an individual convicted of an offence that involves dishonesty, fraud, financial crime or an offence under legislation relating to ML; or that an individual subject to a finding that directly relates to certain crimes will not meet the fitness and propriety requirements, which does not appear consistent with the mandatory requirements set out in the sectoral laws to refuse a licence.. As noted, this framework does not apply to the beneficial owner of a significant or controlling interest in a financial institution, or in the case of someone being an “*associate*” to a criminal. Finally, the GFSC Methodology only applies to new business applications while the C.26.3 requires that authorities should prevent the “*holding*” (not only the “*obtaining*”) of a significant or controlling interest.

273. **Criterion 26.4** – The GFSC’s regulation and supervision of core principles institutions are largely in line with the core principles, including the application of consolidated group supervision for AML/CFT purposes Gibraltar’s regulatory and supervision framework does not differentiate between core principles and non-core principles FIs, including FIs providing a money or value transfer service, and money or currency changing service. The GFSC applies a risk-based approach to supervision. As noted under criterion 26.3, the assessment of the suitability of core principles FIs does not extend to their beneficial owners and others that may exert significant influence.

274. **Criterion 26.5** – Regulation 5 (c) of the SBPR requires supervisory bodies to ensure that when applying a risk-based approach to supervision, they base the frequency and intensity of on-site and off-site supervision on the risk profile of the RFB, and on the risks of ML and TF in Gibraltar. Regulation 7 requires supervisory bodies to take into account the degree of discretion allowed to the RFBs, and appropriately review the risk assessments underlying this discretion, and the adequacy and implementation of its internal policies, controls and procedures. This covers (b) and (c) of the criterion. However, as regards to (a) there is no requirement that the frequency of on-site and off-site AML/CFT supervision be determined on the basis of the ML/FT risks and the policies, internal controls and procedures associated with the institution or group, as identified by

¹¹² A “*notifiable applicant*” is defined as: i Chief Executive Officer; ii Managing Director; iii. Executive Director; iv. Non-Executive Director; v. Managerial Function; vi. Compliance Officer; vii. Money Laundering Reporting Officer; viii. Four Eyes; ix. Trustee; x. Shareholder/Controller (New); xi. Shareholder/Controller (Change); or xii. Other notifiable position.

the supervisor's assessment of the institution's or group's risk profile. However, this is covered by the Financial Crime Methodology and the Financial Crime Procedures Manual adopted by the GFSC, albeit only in the context of the assessment of the residual risk, with impact on the intensity, but not always on the frequency of the inspections for all supervised institutions. Since 2018 the GFSC has introduced a ML/FT risk scoring system of financial businesses subject to its purview, which results in the risk profiling of the FI. This risk profiling is regulated the Financial Crime Methodology, and it is based on a variety of risk factors specific to ML and FT (related to customer, product, interface, country and other risk factors). These factors are used to determine the inherent ML/FT risk of the firm, based on financial crime returns from the firm, which will determine the risk profile of the firm and (but only for those firms that have been already inspected under this new framework) the frequency of their inspections. For firms that have not been inspected under the new framework, supervision is based on general risk which captures financial crime but is not driven by it. The Financial Crime Methodology and procedure do not specifically contemplate the ML/FT risk present in Gibraltar (although, as mentioned, other countries' risk is factored in and product risk, which is only in part driven by the NRAs).

275. **Criterion 26.6** – Regulation 6 of the SBPR requires periodic reviews of the ML and FT risk profile of RFBs and when there are major events or developments in their management and operations.

Weighting and Conclusion

276. The existing legal and regulatory measures are not sufficiently capable to prevent both criminals or their associates from holding or being the BO of a significant or controlling interest, or holding a management function, in a financial institution as, inter alia, they apply only to new and not to already licensed FIs and they do not extend to beneficial owners of a significant or controlling interest. The checks on the source of the funds for controller notifiable applicants are not extended to beneficial owners, which is not in line with the Basel Core Principles. The GFSC has put in place a ML/FT risk-based approach to supervision, but the frequency of the inspections for all supervised institutions is not entirely driven by it. **R.26 is rated PC.**

Recommendation 27 – Powers of supervisors

277. Gibraltar was assessed LC for R.29 in the 2007 IMF report. The report noted the absence of supervision for the *bureaux de change* or the non-bank money remitter. Any outstanding deficiencies related to effectiveness issues are assessed separately from technical compliance under IO.3.

278. **Criterion 27.1** – The SBPR (implementing the POCA) provides the GFSC with the requisite powers to allow it to adequately supervise, monitor and take measures in ensuring that firms are compliant with the legislative and regulatory requirements. These include the power to require all information necessary to conduct effective supervision and to carry out on-site investigations at the premises of relevant Persons (Regulation 11(1)(c)(d)).

279. **Criterion 27.2** – Supervisors have the authority to conduct inspections. The requirement set out under Regulations 11 and 14 of the SBPR (and, more specifically for the GFSC the FS(IG&C) A) allow the GFSC to conduct inspections when required.

280. **Criterion 27.3** – Regulations 12 and 13 of the SBPR permit supervisors to require any relevant information (as interpreted by Regulation 3 of the Regulations) or records from firms as deemed necessary. The GFSC has also powers to require information from firms under Part III of the FS(IG&C) A.

281. **Criterion 27.4** – Regulations 18-21 of the SBPR provide supervisors with the requisite powers allowing them a range of disciplinary and financial sanctions, including the withdrawal, restriction or suspension of a firm’s license due to ML/FT concerns.

Weighting and Conclusion

282. All criteria are met. **R.27 is rated C.**

Recommendation 28 – Regulation and supervision of DNFBPs

283. Gibraltar was rated PC for former R.24 in the 2007 IMF Report. The report noted issues of effectiveness (any outstanding issue of effectiveness is dealt with in the analysis of IO.3) and that no authority had been designated responsibility for monitoring of other DNFBPs.

284. **Criterion 28.1** –

a) (Met) - The Gambling Act 2005 (GA) requires casinos and providers of betting services, both remote and non-remote, to be licensed and it is an offence to offer such services without a licence (SS. 7-15, 23 GA) or to contravene any terms to which the licence is subject (S.4(3) GA).

b) (Partly Met) - Section 3 of the Schedule 1 of the GA provides that a licence to a casino shall be refused if the licensing authority is not satisfied that the applicant for the licence and, where applicable, each shareholder, director of the applicant, each executive manager and interested person is a fit and proper person. “Interested person” is defined in a way that can cover the BO of a significant or controlling interest of a casino¹¹³. Fit and proper is broadly defined with a reference to several standards (not exclusively related to integrity of the applicant), which the licensing authority “may” consider in determining that a person is fit and proper. While among these standards it is included, inter alia, the person’s character, honesty and integrity these factors are not mandatorily required to be considered part of the assessment of the fit and proper. Moreover, when renewing a licence it is not mandatory for the licensing authority to refuse the renewal if it is no longer satisfied either that the licence holder is a fit and proper person to hold the licence or, when the licence holder or any shareholder, director, executive manager or interested person has been convicted of an offence which, in the opinion of the Licensing Authority, affects the fitness of the licence holder to hold the licence (in these circumstances the licensing authority “may” only refuse to renew the licence (par. 7 of Schedule 1)

c) (Met) - The Gibraltar Gambling Commissioner (GGC) is the supervisory authority for the gambling sector in Gibraltar in respect of AML/CFT requirements pursuant to S.29 and 30 of POCA.

285. **Criterion 28.2** – The following have been designated as competent authorities for monitoring and ensuring compliance of DNFBPs with AML/CFT requirements: the Registrar of Supreme Court (RSC)¹¹⁴, for notaries and independent legal professionals; the Office of Fair Trading for dealers in high value goods (which includes dealers in precious metals and stones) and real estate agents;¹¹⁵ the GFSC for TCSPs¹¹⁶, Insolvency Practitioners¹¹⁷ and Auditors¹¹⁸. External

¹¹³ Any person who, if the license were to be granted, would, in the opinion of the Licensing Authority, be able or likely to be able to influence (whether by the holding of securities or otherwise) the conduct of the business of the license holder.

¹¹⁴ The appointment was made on 19/10/2017 through the Proceeds of Crime (Supervisory Authorities) Order 2017 <http://www.gibraltarlaws.gov.gi/articles/2017=205.pdf> through which the RSC was appointed as a Supervisory Authority under Part I of Schedule 2 of POCA.

¹¹⁵ Part I of Schedule 2 to POCA

¹¹⁶ Section 2(1) of the FS(IFS)A sets out that the Authority within the Act is the FSC. Schedule 3 of the FS(IFS)A includes all services defined in Recommendation 22.1(e) relative to TCSPs.

accountants and tax advisors do not have a designated supervisor but fall by default under the Financial Secretary¹¹⁹ are subject to the POCA and are monitored for compliance with these requirements (see table below).

286. **Criterion 28.3** – Section 30(1) of POCA requires that a supervisory authority must effectively monitor the relevant persons for whom it is the supervisory authority and take necessary measures for the purpose of securing compliance by such persons with the requirements of the Act. However, external accountants and tax advisors are not subject to systems for monitoring and ensuring compliance with AML/CFT requirements, as it is required by this criterion.

287. **Criterion 28.4** –

288. As noted under C.28.3, external accountants and tax advisors are not subject to systems for monitoring and ensuring compliance with AML/CFT requirements.

a) The GFSC, OFT and RSC have adequate powers to perform their supervisory functions, including powers to monitor compliance, pursuant to the Supervisory Bodies (Powers etc.) Regulations 2017. Part III of the FS(IG&C)A provides for powers specifically for the GFSC.

b) Section 30 (3) of POCA states that with respect to RFBs referred to in section 9(1)(g) to (i) (with the exception of insolvency practitioners), that is accountants and auditors, real estate agents, notaries and independent legal professionals “*measures taken under this section shall include those necessary to prevent persons convicted of a relevant offence or their associates from holding a management function in, or being a beneficial owner of, those businesses*”. However, except and in part for real estate agents and DPMS, there are no legally enforceable or other measures in place. For TCSP, which are subject to the licensing requirements of the GFSC, see the analysis of C.26.3. The OFT manual for licensing, which applies to real estate agents and DPMS requires, as part of the process to ask for criminal records but only for the “*legal and beneficial owner of the business*”. This process applies to new licensees and not to existing ones.

c) Supervisors of DNFBPs have sanctions available to them in line with R.35 to deal with the failure to comply with AML/CFT requirements, stipulated by the Supervisory Bodies (Powers etc.) Regulations 2017.

289. **Criterion 28.5** – Regulation 5 of SBPR requires supervisory bodies to use a risk-based approach, in supervision. However, except for DNFBPs supervised by the GFSC and the GA supervision is not performed on a risk sensitive basis.

a) (Partly Met) – Regulation 5 (2) (c) of the SBPR requires supervisory authorities to base the frequency and intensity of on-site and off-site supervision on the risk profile of the RFB, and on the risks of ML/FT in Gibraltar. However, this is not performed for all DNFBPs.

b) (Partly Met) – For DNFBPs subject to the GFSC, see analysis of criterion 26.5 For all DNFBPs, in addition to Regulation 5 mentioned above, Regulation 7 requires supervisory to take into account the degree of discretion allowed to the RFBs, and appropriately review the risk assessments underlying this discretion, and the adequacy and implementation of its internal

¹¹⁷ Section 2(1) of the Insolvency Act 2011 lists the FSC as the Authority/Commission responsible for Insolvency Practitioners

¹¹⁸ Section 2A(1) of the Financial Services (Auditors) Act 2009 appoints the FSC as the designated Authority responsible for the supervision of Auditors.

¹¹⁹ In the absence of a prescribed supervisory authority the default supervisory body for any relevant financial business is the Financial Secretary under S29(2) of POCA (See schedule 2 for a list of supervisory bodies that have been prescribed and Paragraph (e) which specifies the Financial Secretary for any relevant financial business not covered by other supervisory bodies).

policies, controls and procedures for DNFBPs within the remit of the GFSC see analysis of criterion 24.5. However, this is not performed for all DNFBPs.

Weighting and Conclusion

290. For casinos, existing measures are not sufficiently capable to prevent both criminals and their associates from holding or being the BO of a significant or controlling interest, or holding a management function, in a casino. Except and in part for real estate agents and DPMS, there are no legally enforceable or other measures in place to prevent criminals or their associates from being professionally accredited or holding (or being the beneficial owner of) a significant or controlling interest, or holding a management function, in a DNFBPs. Although the majority of DNFBP types are subject to systems for monitoring and ensuring compliance with AML/CFT requirements, no such systems for external accountants and tax advisors. Although required by the legal framework, supervision is performed on a risk sensitive basis not for all types of DNFBPs. **R.28 is rated PC.**

Recommendation 29 - Financial intelligence units

291. In the 2007 IMF assessment report Gibraltar was rated LC with former R.26. The main deficiencies were: absence of a clear public record of GFIU's functions; the Gambling Ordinance allowed for the Gambling Commissioner, not the GFIU, to decide to disseminate copies of the disclosures it receives to law enforcement authorities; the legal requirements for STRs relating to financing of terrorism were confusing; the circumstance and extent to which the GFIU could and would obtain additional information from reporting businesses were not clearly delineated, so that judgments could be made by counsel for REs on a case-by-case basis as to whether the GFIU staff was over-reaching.

292. **Criterion 29.1** – The GFIU is a statutory body assigned to collect, store, analyse and disseminate intelligence related to criminal conduct and act as the recipient for disclosures of suspicious transactions (POCA section 1C (a, b)) within the meaning of R.29. The Head of the GFIU is responsible for the attainment of the functions set out in section 1C. The GFIU also provides strategic analyses addressing ML/FT trends and patterns and disseminates the results of its analyses (POCA section 1D (a, b)). The GFIU is staffed by officers seconded from HM Customs and the RGP and the GFSC. In addition, as part of a restructure of the unit there are Civil Service staff members who are employed within the GFIU as permanent members for administrative matters. Since 2004, the GFIU has been a member of the Egmont Group of Financial Intelligence Units.

293. **Criterion 29.2** –

a) The GFIU serves as a central agency in Gibraltar for the receipt of disclosures filed by REs. It acts as a recipient for disclosures of suspicious transactions under the relevant applicable legislation as required by R.20 and R.23 (S.1C (b) of POCA). ML SARs are disclosed by REs to the GFIU, a police officer, a customs officer or a nominated officer (S.4G of POCA). FT SARs must also be disclosed to the GFIU (S.40 of the 2018 TA). Under R99 of the GFSC anti-money laundering and terrorism financing guidance notes (AMLGNs) it is stated that GFIU is the authority to whom all STRs should be addressed to. As regards the gambling industry, licence holders are obliged to submit a STR directly to the GFIU (GGC's revised Code of Practice for the Remote Gambling Industry (par.4.16)). The OFT's AMLGNs for high value dealers (HVDs) and real estate agents (REAs) clearly indicates that all disclosures are to be submitted to the GFIU.

b) The legislation does not require reporting cash or threshold transactions and wiring transfers. Gibraltar operates a system of border cash declarations (see R.32). HM Customs and the GFIU have in place an electronic mechanism for the exchange of information regarding cash declarations reports. Cash declaration reports are inputted into GFIU's databases.

294. **Criterion 29.3 –**

a) Under POCA (1DA (b, 5) and 1ZDA) RFBs must provide the additional information requested by the GFIU following a report (including, but not limited to, a disclosure or suspicious activity report in accordance with this or any other enactment).

b) According to the authorities, the GFIU has direct electronic access to a broad range of information and databases (e.g. ID Cards, Driving Licences, Vehicle Registration, Companies House and UBO, Cyclops, Interpol), including information on previous convictions. The authorities also reported that access to the HMC and GFSC databases can be obtained on request without delay.

295. **Criterion 29.4 –**

a) and b) The POCA (s.1D (a, b)) provides that the GFIU must undertake operational and strategic analysis based on the information received from REs and the other information available to it. The GFIU may obtain information from a financial institution, defined as a 'RFB' (S.9 of POCA), through the use of a Data Request Form (Schedule, Part 1, par.2(1) of the 2004 Data Protection Act), provided that the information is for the following purposes; the prevention or detection of crime; the apprehension or prosecution of offenders; or the assessment or collection of a tax or duty or an imposition of a similar nature.

In addition, according to POCA (1DA) the GFIU has the power to request additional information upon receipt of a report (including, but not limited to, a disclosure or SAR in accordance with this or any other enactment) and when it reasonably considers that, for the proper fulfilment of any of its functions (S.1C of POCA), it is necessary or expedient to seek additional information from any relevant person who is mentioned in or otherwise identifiable from the report, or to the reasonable knowledge or belief of the GFIU, holds information that is relevant to analysis of the report.

The GFIU analyses all STRs received through its online system followed by a grading method conducted by an experienced Financial Intelligence Officer (FIO) and if further work is required operational analysis is conducted by other FIOs. A strategic analysis was conducted in 2017 for internal use, while the 2018 strategic analysis STRs is being finalised.

296. **Criterion 29.5 –** The powers of GFIU to disseminate information to the competent authorities, both national and other FIUs are defined in POCA (section 1(B)(4), 1C(a and c) and 1E(1)). Also, when the GFIU in the performance of its functions has reasonable grounds to suspect that a RFB, or any other person, has engaged in conduct which is prohibited by law or contravenes any regulatory standards, the GFIU, if it considers it appropriate to do so, may refer the matter to the RGP, HM Customs, the Income Tax Office or a supervisory body listed in Part I of Schedule 2 of POCA, as appropriate (1M of POCA). POCA (1K(a)) also provides that LEAs are entitled to information held by the GFIU only if the Head reasonably believes that such information is required to investigate suspected criminal conduct. The authorities explained that the Head of GFIU should take reasonable procedural arrangements and impose such reasonable safeguards regarding the furnishing of information as the Head considers appropriate to maintain the confidentiality of that information.

297. The GFIU disseminates information and the results of its analysis (e.g. the subject of the STR, related account details and the nature of the suspicion as well as any additional information that has been collected) to relevant competent authorities (e.g. RGP, HMC, ITO or GFSC) through a 3x5x2 intelligence report system which is an internal system within the Suspicious Activity Reporting (SARs) online system Themis. As regards foreign FIUs the GFIU uses the Egmont Secure Web for intelligence and investigation purposes.

298. **Criterion 29.6 –**

a) The POCA (section 1K, 1IC, 1L) provides for the security and confidentiality of information, including procedures for handling, storage, dissemination, and protection of, and access to, information. In addition, the GFIU has a Protective Marking Scheme Policy in place, which protects documents and provides advice on handling, storage and access. Training and monitoring of access to and use of GFIU's data by end-users is conducted when new staff joins the GFIU. All STR information is handled at the 'Official-Sensitive' level within GFIU.

b) The GFIU staff is locally vetted by the RGP and signed the Official Secrets Act. Vetting is conducted as a matter of policy within all Government departments. Furthermore, RGP officers seconded to the GFIU are vetted by UK Security Vetting Agency to SC(E) and DV level.

c) Access to the GFIU facilities is restricted to staff with the use of key fobs, a physical key and an alarm system that is connected to the police Command and Dispatch. The system is serviced and maintained by a security company. Access to data is restricted to individual users having usernames and passwords. The GFIU also applies the Egmont recommendations on security as defined in the 'Securing a Financial Intelligence Unit' Operational Guidance document.

299. **Criterion 29.7 –**

a) According to POCA (section 1B (3, 4) and 1C) the GFIU is operationally independent and autonomous and has the authority and capacity to carry out its functions freely. The GFIU falls under the Ministry of Justice for budgetary/administrative/HR matters and it is physically located in a dedicated building outside the parent organisation.

b) According to POCA (section 1B (4), 1C(c), 1E, 1GA) the GFIU is able to engage independently with local competent authorities and foreign law enforcement agencies as well as FIUs. The GFIU does not legally require a MoU for the exchange of information with other FIUs, although as an Egmont member it has signed MoUs with other countries which are required by their laws to do so (Chile in 2008, San Marino, Japan, South Africa, Australia, Poland and Israel in 2014, Panama in 2015, and Canada and the Holy See in 2017).

The GFIU has also signed MoUs with the OFT, GGC, GFSC, ITO and Friendly Societies.

c) The GFIU falls under the Ministry of Justice for budgetary/administrative/HR matters, but it operates autonomously and independently for all operational matters (see sub-criterion (a)).

d) The legal basis in place allows GFIU to operate freely of any undue influence or interference which might compromise its operational independence. The GFIU can obtain and deploy any resources needed to carry out its functions upon request to the Ministry of Justice. This is also confirmed by the approval of relevant requests made during the review period.

300. **Criterion 29.8 –** The GFIU has been a member of the Egmont Group since 2004.

Weighting and Conclusion

301. All requirements are in place. **R.29 is rated C.**

Recommendation 30 – Responsibilities of law enforcement and investigative authorities

302. In the 2007 IMF Report, Gibraltar was rated compliant in respect of these requirements.

303. **Criterion 30.1** – The RGP, the police force of Gibraltar is responsible for the investigation of ML associated predicate offences and FT (ss.11 & 26 Police Act 2006).

304. The RGP has operational capabilities across a range of areas such as the Drug Squad, the Criminal Investigation Department (CID) and the uniformed branch. All may investigate proceeds generating crime. To meet the risk of ML through the finance industry and other areas of the economy, given Gibraltar's position as a financial centre, in May 2016 the Economic Crime Unit (ECU) of the RGP was restructured into two units: the Money Laundering Investigation Unit (MLIU) and the Fraud Squad. Any ML or parallel financial investigation is carried out by the MLIU. The RGP has a Special Branch (SB) department which is responsible for CT investigations. FT investigations are conducted jointly between SB and the MLIU. The 2017/2018 Annual Policing Plan produced by the GPA sets objectives and targets which include "*The RGP will pro-actively conduct investigations into terrorist funding and the facilitation of terrorism through other means*", "*The RGP will increase detections of ML offences*."

305. HMC is responsible for the collection of import and export duties. The Imports and Exports Act (I&EA) 1986 defines HMC's role and responsibilities. HMC is primarily concerned with the movement of goods and cash, in and out of Gibraltar and the licensing, sale, storage and transportation of tobacco. The offences that HMC investigates are drawn from the I&EA and subsidiary legislation such as the Imports and Exports (Control) Regulations, which also lists prohibited and restricted goods. It is because of these goods that HMC will also count on other legislation like the CA in order to prosecute offences connected with the importation of such goods, e.g. the possession and intent to supply of controlled drugs.

306. The Office of Criminal Prosecutions and Litigation (OCPL) provides legal advice and expert assistance to LEAs in the course of investigations, including those involving ML or FT.

307. **Criterion 30.2** – Law enforcement agencies tasked with investigating predicate offences in Gibraltar are specified at 30.1 above. Any ML or parallel financial investigation is carried out by the MLIU. FT investigations are conducted jointly between SB and the MLIU. Parallel financial investigations are conducted regardless of where the predicate offence occurred. HMGOG produced an AML/CFT Strategy which lays out the policy for LEA's to conduct parallel financial investigations for major proceeds generating crimes ("*The conduct of parallel financial investigations will be pursued by the MLU as a matter of policy with a view to identifying and confiscating both the proceeds of criminal activity as well the instrumentality through which the crime was committed*"). Furthermore, this has led to the development of Standard Operating Procedures in the RGP and HMC for the instigation of parallel financial investigation's (RGP015/RGP018 and HMC010 refer).

308. **Criterion 30.3** – The RGP and HMC are empowered to identify, trace and initiate the freezing and seizing of property that is, or may become, subject to confiscation, or is suspected of being proceeds of crime. Within the RGP these tasks are conducted by the MLIU. The detection of crime includes the detection of the proceeds of crime. POCA Section 58 3A (a) and (b) allows for a restraint order to be obtained if a Court is satisfied that a criminal investigation has been initiated and there are reasonable grounds to suspect that the alleged offender has benefited from his criminal conduct. This criminal investigation can only be commenced by an LEA and therefore all subsequent executive actions will be conducted by the RGP and HMC to identify, trace and initiate freezing and seizing of property that is or may become subject to a confiscation or is suspected to

be the proceeds of crime. Within HMC the identification, freezing and seizing of property that is or may become subject to a confiscation is the responsibility of the Investigation Branch (IB). The Collector of Customs will decide the structure of his organisation and the division of work within it without the requirement of an Act.

309. **Criterion 30.4** – As set out above the RGP is in charge of conducting financial investigations, ML investigations and FT investigations in Gibraltar. HMC is primarily concerned with the movement of goods and cash, in and out of the jurisdiction. The offences that HMC investigates are drawn from the I&EA and subsidiary legislation. HMC will also investigate associated ML offences.

310. Other competent authorities (such the GFSC, the Commissioner of Income Tax and the GDP) assist in combatting ML and FT by the exchanging of information in a joint agency approach.

311. **Criterion 30.5** – The RGP conducts any bribery or corruption investigations. The RGP would investigate any ML/FT offences, arising from, or related to corruption offences. No separate specialised unit deals with corruption in Gibraltar. The criterion is therefore not applicable.

Weighting and Conclusion

312. All criteria are met apart from 30.5 which is not applicable. R.30 is rated C.

Recommendation 31 - Powers of law enforcement and investigative authorities

313. In the 2007 IMF Report, Gibraltar was rated compliant in respect of these requirements.

314. **Criterion 31.1** – The competent authorities conducting investigations of ML/FT and associated predicate offences are able to obtain access to all necessary documents and information for use in those investigations and in prosecutions and related actions through various provisions

a) Production or disclosure orders enable the obtaining of records and information held by natural and legal persons, FIs and DNFBPs when investigating predicate offending, ML or FT (POCA 149, 151, 161, 167, 174) For FT investigations the Terrorism Act 2018 provides for restraint orders (s. 60) account monitoring orders (s. 81 and Schedule 8) the searches of premises (s. 79) and customer information orders (s. 80 and Schedule 7.). Warrant may be obtained under s. 12 CP&EA authorising police officers (and customs officers) to search premises and potentially seize and retain anything for which a search has been authorised. The materials which cannot be seized by LEA's under s.12 are items subject to legal privilege, excluded material or special procedure material. Section 13 enables the police officer an access to excluded material or special procedure material for the purposes of a criminal investigation upon approval of an application made to a judge or magistrate.

b) Persons and premises can be searched. Search warrants for premises are regulated under CP&EA (s.12, Schedule 1), POCA (s. 156), Drug Trafficking Offence Act (DTOA) – s. 61, among others. Under s. 12 CP&EA police officers (and customs officers) may search premises and potentially seize and retain anything for which a search has been authorised. The materials which cannot be seized by LEAs under s.12 are items subject to legal privilege, excluded material or special procedure material. Section 13 enables access to excluded material or special procedure material for the purposes of a criminal investigation on application to a judge or magistrate (see also 31.1 a)). CTA Section 17 (1) allows a Police officer to enter a business premises at a reasonable time to inspect and take copies of material relevant to an investigation. If there is a belief that items may be removed, destroyed or tampered with, a person has failed to comply then a search warrant can be obtained under Section 18 (CTA). POCA Section 116 allows for the search of premises, a vehicle and a person for cash where no offence is disclosed if there are reasonable

grounds to suspect that there is cash which is either recoverable property (i.e. the proceeds of unlawful conduct) or cash to be used in unlawful conduct and that the cash is over GBP 1,000. POCA Section 117 requires Section 116 to be exercised with prior approval of a magistrate or, if not available, a senior officer (with regards to the Police this will be an Inspector or above; and a Senior Customs Officer or above for HMC). Powers to search persons derive from various Acts. Powers to stop and search a person are found in CP&EA Section 5 but are limited to the search for bladed articles, stolen property or articles to be used in burglary, theft, taking a conveyance, fraud or damaging property. The CA Section 523 (2) (a) gives powers of search for controlled drugs. Further powers of search of a person exist in the TobA Section 17D.

c) The power to obtain witness statements derives from the CP&EA Sections 186 and 187. Law enforcement officers have the power to take statements. Witness statements are voluntary in nature and no person can be forced to supply a witness statement to the police. Obligation to give a statement at the court is regulated by CP&EA S.183 (1)b) which states that *if a magistrate is satisfied that person will not voluntarily attend as a witness or will not voluntarily produce the document or thing, the magistrate must issue a summons directed to that person requiring him to attend before the court at the time and place appointed in the summons to give evidence or to produce the document or thing.*

d) Law enforcement officers have the power to seize and obtain evidence. CP&EA (s.25) gives a general power to seize anything for which they have 'reasonable grounds for believing' that:

- i. has been obtained in consequence of the commission of an offence, or;
- ii. is evidence in relation to an offence being investigated or any other offence, and in either case;
- iii. provided that it is necessary to seize it in order to prevent it being concealed, lost, damaged, altered or destroyed.

The powers of seizure under this section are in addition to those conferred by any similar law but does not authorise the seizure of items subject to legal privilege S13.(1) authorize police officer to obtain access to excluded material or special procedure material (which include legal privilege) for the purposes of a criminal investigation by making an application to a judge or magistrate (see also EC 31(1)).

TA2018 Section 87(3) and 87(5)(b) allows a police officer to seize and retain evidence found during a search under Sec 87(1) and 87(4). Furthermore, TA2018 Section 88(3)(a) allows for the seizing and retaining of evidence found during a search of a vehicle conducted under Section 88(2).

315. **Criterion 31.2 (Partly Met)** – The competent authorities are able to use a wide range of investigative techniques for investigating ML, associated predicate offences and FT.

a) The authorities advised that using undercover officers from UK police forces and/or military personnel for actions in Gibraltar had taken place. Plain clothed officers and Covert Human Intelligence Sources (CHIS) are both regularly used by LEAs. Neither are regulated by legislation though both RGP and HMC have written CHIS policies and any use of undercover officers must not involve entrapment in accordance with the principles set out by the House of Lords case of *Loosley, Att-Gen's Reference (No. 3 of 2000)* [2002] 1 Cr.App.R. 29 which took account of the jurisprudence emanating from the European Court of Human Rights in *Teixeira de Castro v. Portugal*, 28 E.H.R.R. 101.

b) The LEAs are currently unable to intercept communications.

c) Powers to permit the production and seizure of computerised information are provided in CP&EA (s. 26) and POCA (ss.153, 159.)

d) Controlled delivery is permitted under TOCA (s.13.) when investigation is carried out for an offence punishable in Gibraltar by imprisonment for a term of four years or more.

316. **Criterion 31.3 –**

a) and b) Authorities advised that the LEAs use a number of tools to identify the assets held by the subject of an investigation. None of these methods requires that the owner be notified. Although the LEA might not be the custodian of the data, on occasions it will have direct access to the database or may readily request it under Schedule 2, Part 1, Section 2 of Data Protection Act (DPA). Many of these databases will not only hold specific information on the assets held by an individual, such as vehicles, vessels, companies/businesses and properties, but will themselves create links, through registered names and addresses, to other individuals concealing the assets on their behalf. Banking institutions are bound by the restrictions of the DPA in terms of the processing of data for purposes other than what the data was obtained for. However, the DPA allows for a number of exceptions under Schedule 2 Part 1 Sec 2 (1)(a) and (b) to the processing of data other than for the purpose it was obtained. Two of these exceptions are for the prevention or detection of crime and for the apprehension or prosecution of offenders. The timeliness of the response from FIs is governed by POCA Sec 30B (1) which requires a financial institution to have systems in place to allow for a full and speedy response to LEA requests as to whether they maintain or have maintained a business relationship with a specified person in the 5 years prior to the request. If the financial institution does not wish to divulge the information LEAs have the power to apply to a Judge for a Customer Information Order under POCA sec 167 for ML, confiscation and civil recovery investigations.

317. The TA2018 Section 80 and Schedule 7 allow a police to obtain a Financial Information Order. This enables a police officer to identify whether a natural or legal person holds or controls an account within a financial institution. Section 81 and Schedule 8 allows for an account monitoring order to be obtained that will allow for real time asset movements on an account to be monitored. These powers can be applied only when the criminal offences provided in the TA 2018 are concerned. Neither of these applications requires the notification of the holder of the account in question.

318. **Criterion 31.4 –** The competent authorities investigating ML, associated predicate offences and FT are able to ask for all relevant information held by the FIU and may use such information as intelligence to further their investigations. The function of the GFIU is to exchange information regarding criminal conduct with other FIUs, other similar bodies and law enforcement agencies within and outside of Gibraltar (POCA (S. 1C(c))).

Weighting and Conclusion

319. Whilst Gibraltar, to a large extent, has empowered law enforcement to investigate ML/FT and associated predicates but the investigative means of intercepting telephone communications is not regulated by statute and is not permitted by law. **R.31 is rated LC.**

Recommendation 32 – Cash Couriers

320. In the 2007 IMF assessment report Gibraltar was rated NC on SR IX. The main technical deficiencies included: lack of a declaration or disclosure system in place; partial measures for seizure and confiscation of currency suspected to be related to drug trafficking.

321. **Criterion 32.1** – Gibraltar has a declaration system in place. Any person has to submit a cash declaration entering or leaving the EU via Gibraltar (EU Regulation 1889/2005). The 2017 amendment to the Imports and Exports Act transposed the provisions of the aforementioned Regulation. However, this does not apply to passengers travelling to or from another EU member state. All entry points (airports/marinas/ferry terminals) potentially receiving passengers from destinations outside the EU have been installed with appropriate signs and provide the adequate forms. Additionally, all yachts arriving in Gibraltar have a legal requirement under the Port Rules (s.7B) to complete a pre-arrival notification. For outgoing mail packages, the Royal Gibraltar Post Office personnel are trained to discourage individuals from sending high value goods or currency through the mail. Notwithstanding, should the person insist in sending the item, a CN23 declaration form for items over GBP 270 must be completed. The I&EA laws will still be applicable and large amounts of cash would be referred to HMC. Should such commodities be transported in cargo, they have to be declared through a manifest and cleared through a Single Administrative Document (SAD).

322. **Criterion 32.2** – All persons making a physical cross-border transportation of currency or BNIs, which are of a value exceeding a threshold of EUR 10,000, are required to submit a truthful declaration to the designated competent authorities. Gibraltar possesses a written declaration system, which applies to any natural person entering or leaving the EU borders carrying amounts equal to or greater than the aforementioned threshold. The Imports and Exports Act (I&EA) (section 91E (1)) indicates, that a declaration under Art.3 of the European Regulation (1889/2005) must be made in writing and in such form as has been approved by the competent authority. In accordance with the Regulation (Art.3), the obligation to declare shall not have been fulfilled if the information provided is incorrect or incomplete.

323. **Criterion 32.3** – This criterion is not applicable since Gibraltar has a declaration system.

324. **Criterion 32.4** – In accordance with the I&EA (section 91F (1)), for the purposes of ensuring compliance with the European Regulation (1889/2005), a customs officer may require information from a person to determine, whether that person is concerned with the importation or exportation of cash for which a declaration is required; and whether a declaration has been made. Additionally, section 91F (2) of the I&EA provides for sanctions to any person who dishonestly withholds substantive information or misleads the officer when providing such information. Also, a customs officer may seize and detain cash being imported into or exported from Gibraltar for up to 48 hours if the person importing or exporting that cash has not complied with his obligations under Article 3 of the European Regulation (obligation to declare) (section 91K (1) of the I&EA). If the officer is still not convinced of the true origin of the currency or BNI and its intended use, section 91K (4) of I&EA states that the officer can then make an application for an order under section 120(4) of POCA and the judge, magistrates' court or the Supreme Court may extend the detention beyond 48 hours and up to a maximum of 2 years.

325. **Criterion 32.5** – The I&EA (section 91L (1)) stipulates that a false declaration or failure to declare is subject to an administrative fine up to 10% of the undeclared amount. The amount is determined by the Collector of Customs. This penalty cannot be considered proportionate or dissuasive. Also, section 91F (2) provides that a person is liable on summary conviction to imprisonment for a period not exceeding six months or a fine not exceeding level 4 on the standard scale. This is applied in the case where a person withholds substantive information or misleads a customs officer.

326. **Criterion 32.6** – Section 910 (1) of I&EA states, that the competent authority shall collect and exchange information with the GFUI. HM Customs and the GFUI have an electronic mechanism in place for the exchange of information regarding cash declarations reports made at entry points,

as well as cash confiscations. This has been incorporated within the new online SAR reporting system and the information is inputted directly into the GFIU's database. Scanned copies of the declaration form and any attached documents are sent for all declarations whether suspicious or not. These are accompanied by any additional reports prepared by HMC.

327. **Criterion 32.7**– The customs authorities in Gibraltar co-operate with the Borders and Coast Guard Agency (BCA) on issues related to the implementation of Recommendation 32 on the basis of Memoranda of Understanding. The BCA has responsibility for immigration and security matters at both the Cruise/Ferry Terminal and the Gibraltar International Airport. It is tasked with passenger screening at the Cruise/Ferry Terminal and Airport, and such activity might result in the detention of cash and other forms of contraband. Detections are immediately referred to HMC for appropriate action to be taken.

328. Both public and private marinas are the responsibility of the HMC Marine Section which currently concerns itself with yacht clearance and sea patrols there. It can also count on the assistance of the land based HMC Outfield patrol crews who actively visit marinas as part of their duties to monitor all general areas and coastlines.

329. Customs officers at all entry points are trained to deal with cash seizures and declarations and refer such cases to the Investigation Branch, which in turn reports to the GFIU as in C.32.6.

330. **Criterion 32.8** – According to I&EA (section 91K (1)), upon discovering a false declaration or a failure to declare, the HMC Officers may seize and detain cash for up to 48 hours. HMC and the RGP have the authority to stop currency and BNIs whether there is a suspicion of ML/FT or predicate offences. In accordance with the POCA (section 119(1)), a customs officer or a police officer may seize any cash if he has reasonable grounds for suspecting that it is recoverable property or intended by any person for use in unlawful conduct. While the customs officer or police officer continues to have reasonable grounds for his suspicion, cash seized may be detained initially for a period of 48 hours. If a detention period (initiated in accordance with I&EA or POCA provisions) longer than 48 hours is justified, then the Court may grant an order for the continued detention of the cash under conditions indicated in POCA. The minimum amount that can be seized under section 119 POCA is currently GBP 1000.

331. **Criterion 32.9** – Customs Authority's database includes all cases of declarations that amount to or exceed the prescribed threshold (EUR 10,000). Whenever there is a false declaration or suspicion of ML/FT, this entry is linked to any further investigations and/or result, whether an administrative penalty, a conviction(s) and/or a confiscation(s). The aforementioned information is available through the mechanisms detailed in Recommendations 36 to 40 (most often through the FIU or the Judiciary). Section 910 (1b) additionally stipulates that HMC shall collect and exchange information with the competent authorities appointed by Member States for the purposes of and to the extent required by the European Regulation.

332. **Criterion 32.10** – The proper use of data and information collected through the Gibraltar declaration system is regulated by the Data Protection Act, which sets the principles and safeguards with respect to data storage and processing (section 910 (2) of the I&EA). There is nothing to suggest that these safeguards would restrict trade payments or the freedom of movement of capital.

333. **Criterion 32.11** – Individuals, who are carrying out physical cross-border transportation of currency or BNIs, related to a ML/FT or a predicate offence, are subject to criminal sanctions for those offences. As indicated in R.3, persons guilty of a ML offence are liable on summary conviction to imprisonment for a term not exceeding six months or a fine not exceeding GBP 10,000 and on conviction on indictment to imprisonment for a term not exceeding fourteen years or to a fine or to both (section 2-4 of the POCA). As highlighted in R.5, a person guilty of a FT offence is liable on

summary conviction, to imprisonment for a term not exceeding six months or to a fine not exceeding GBP 10,000 and on conviction on indictment, to imprisonment for a term not exceeding fourteen years or to a fine or to both; (section 35-39 of the TA2018). This is in addition to the possible penalties for providing a false declaration. The sanctions can be considered proportionate and dissuasive.

334. Measures consistent with R.4 enable the confiscation of currency or BNIs.

Weighting and Conclusion

335. Gibraltar possesses a declaration system for incoming and outgoing cross-border transportation of currency and BNIs. Potential gaps have been identified: a) The declaration system applies only to movements (both inward and outward) of cash and BNI from and to the EU; b) Penalties for failure to declare cannot be considered proportionate or dissuasive. **R.32 is rated LC.**

Recommendation 33 – Statistics

336. In the 2007 IMF assessment report Gibraltar was rated PC with former R.32, due to lack of complete and detailed statistics in several areas, among them prosecutions and convictions, disclosures, MLAs, cash seizure and forfeiture.

337. **Criterion 33.1** – Gibraltar authorities have been using the OSCE data collection model as the basis to provide a consolidated and comprehensive view of relevant data regarding AML/CFT. The authorities collect statistics in particular on:

(a) STRs, received and disseminated: STRs received by the FIU can be broken down by sectors (REs) and underlying offence (ML/FT only or predicate offences); STRs are analysed and disseminated by the GFIU. A distinction is made in the statistics which are disseminated to LEAs and those disseminated to a government authority or regulatory body. Recipient bodies also maintain their own statistics of receipts of STRs.

(b) ML/FT investigations, prosecutions and convictions; The provided dataset contains combined statistics from LEAs on ML and predicate offence investigations, including data on convictions and prosecutions (number of cases/individuals). FT cases are the remit of the RGP. The RGP and HMC are the only two bodies who can bring prosecutions to the Director of Public Prosecutions hence the dataset provided by these two bodies is complete.

(c) Property frozen; seized and confiscated; The RGP is responsible collating data on the freezing, seizing and confiscating property whether in relation to ML/FT or confiscation post-conviction (restraint, confiscation, forfeiture). The Gibraltar authorities maintain combined (HMC and RGP) statistics on assets frozen, seized and confiscated, which can be broken down to underlying offences. HMC and the RGP are the only two bodies who are responsible maintaining and providing these statistics.

(d) Mutual legal assistance or other international requests for cooperation made and received. Statistics on incoming and outgoing requests are provided by HMC and the RGP (combined) and separately by the GCID and the GFIU. Mutual Legal Assistance incoming and outgoing requests and extradition requests are recorded on a separate datasheet. Among others, statistics include information such as status (whether or not it is actioned), time taken to execute (incoming), underlying offences committed or suspected, country of origin – most popular originators/recipients of requests. Gibraltar maintains records on its extradition requests. The data provided to the evaluators by the country includes all received and sent MLA requests.

Weighting and Conclusion

338. Criterion 33.1 is met. **R.33 is rated C.**

Recommendation 34 – Guidance and feedback

339. Gibraltar was rated PC with former R. 25 in its 2007 IMF report. The existing guidance at the time did not address the techniques or methods associated with FT; no feedback or guidance had been provided to *bureaux de change*, the stand-alone money transmitter, nor to most DNFBP sectors.

340. **Criterion 34.1** – Supervisors are required to establish effective and reliable mechanisms so that individuals or firms may disclose any breaches of POCA (Section 6A, POCA). According to the Gibraltar authorities this breach reporting includes STR disclosures.

341. The GFSC issued Guidance Notes in support of POCA (AMLGN), in which Chapter 8 gives details on reporting, including STR disclosure, and also specific guidance for DLT providers, including guidance on the application of AML/CFT requirements. This is further supplemented by Guidance Notes specific to support the Counter Terrorism Act that the GFSC issued in 2010.

342. In November 2017 the GFSC issued all *bureau de change* and consumer credit firms, a “Dear CEO letter” setting out high level guidance of POCA requirements.

343. There is a guidance specifically issued for the Audit Profession (SGAP) and DLT Sector and RSC has issued AML/CFT Guidelines for Legal Professions.

344. The OFT has issued AML/CFT Guidance Notes for High Value Dealers (HVDs) (OFT001) and for Real Estate Agents (REAs). Additionally, the OFT has issued Beneficial ownership guidance notes for HVDs and REAs (OFT019) and sample CDD forms, letters, emails, presentations and seminars.

345. The GGC has published an AML Code in 2011 that has undergone various updates including a recent update in 2018 following changes to POCA due to the implementation of 4AMLD, which is dedicated specifically to the remote gambling sector with the Code for the land-based sector also being revised.

346. The FIU has issued a document that provides guidance to REs on AML/CFT and the policy (GFIU003-SAR Quality Policy) to enhance the quality of the STRs by informing the reporter through a feedback system of any shortfalls identified within the STR content/context or where SARs are not of the required standard.

347. Project Nexus, coordinated by the FIU, was launched in 2017. It is a multi-agency outreach programme, where feedback is two way, with the REs requested to submit their feedback on the quality of the delivery, subjects, speakers and venue used.

348. The NCO has also issued three Newsletters (FT Risks in the NPO sector and a second one on the changes to POCA post the transposition of 4MLD, a third on the new Terrorism Act 2018 and a fourth one on the publication of the new Sanctions Act).

349. As for feedback from the GFSC, following a full risk assessment of a firm, regardless of the scope of it, feedback will be provided to firms on an exceptions basis only i.e. FIs will not provide firms with its assessment of the firm’s systems and control. Nonetheless, it will provide comments, recommendation, requirements for actions, etc. where it does not consider that the firm’s systems of controls meet legislative or regulatory requirements, or where the systems of controls are considered inadequate.

Weighting and Conclusion

350. All criteria are met. **R.34 is rated C.**

Recommendation 35 – Sanctions

351. Gibraltar was rated LC with the previous R.17. The report noted that Bureaux de Change and money transmitters are not subject to adequate sanctions. A range of supervisory sanctions apply for the TCSP and internet-based gambling sector, but few for the land-based casino or other DNFBP entities. All REs are now subject to sanctions.

352. **Criterion 35.1** – The 2019 Sanctions Act (Part II par.7(1, 4) and Part II par.9(1, 2)) provides for a range of sanctions for TFS breaches. The Act (Part V par.51(1, 2)) provides both for fine not exceeding level 5 (set at GBP 10.000) or/and imprisonment up to 10 years for a person who commits an offence for which no separate penalty is provided. Such sanctions are also available for corporate bodies and their officers-managers-directors. Criminal sanctions are available for the purposes of preventing prohibitions or requirements from being circumvented (2019 Sanctions Act, Part III par.33(6)).

353. As regards the NPO sector, the Charities Commissioner and the RFS have access to a range of sanctions for failing to comply with relevant requirements. See analysis at C. 8.4(b).

354. There is a wide range of sanctions under POCA (criminal) for specific requirements established by POCA and the 2017 Supervisory body regulation (SBPR) Act. In particular, a supervisory authority it is satisfied that the relevant person under its supervision has defaulted or breached its obligations under POCA or any applicable law or guidance (R.18).

355. There are criminal and administrative sanctions available for non-compliance with FATF Recommendations 9 to 23. The POCA (Part II S.33) provides for criminal sanctions for all breaches, except for correspondent banking with a non-EEA institution (S19 POCA); PEPs (S20, 20A and 20B POCA); reliance on third parties (23 and 23A POCA); and risk assessment (25A), where only administrative sanctions apply. However, there are few instances where certain requirements, created solely by the AMLGN, are not enforceable. The most significant concern the requirement for firms to undertake the risk assessment for new products, business practices, delivery mechanisms and developing technologies (for both new and existing products) prior to the launch of these (R21); the requirement to “understand” the purpose and intended nature of the business relationship (R60); the requirement to take into consideration whether the respondent institution had been subject to any ML/TF investigation or regulatory action¹²⁰.

356. In addition, administrative sanctions are available under the 2017 Supervisory Bodies (Powers etc.) Regulations. The administrative sanctions provided are twice the amount of benefit derived from a default or breach of the applicable law or guidance where that benefit can be determined; or EUR 1 million. Higher penalties are applicable where a RFB is a credit institution or a FI; in this case a supervisory body may impose a penalty not exceeding EUR 5 million or 10% of the total annual turnover, according to the latest available accounts approved by the management body in the case of a legal person; and EUR 5 million in the case of a natural person. These sanctions appear to be proportionate and dissuasive.

¹²⁰ Another issue concerns Article 9 and Article 13 of the WTR, which provides that the intermediary service provider and the beneficiary’s PSP (not the payer’s service provider) should consider missing or incomplete information on the payer of the payee (rather than all information) when assessing if a transaction is suspicious and whether it is to be reported to the FIU. This issue is addressed by R34C of the AMLGN which states that when a PSP acts for both the payer and the payee it should take into account all information in order to determine whether disclosure to the FIU is required and also, if applicable, file a report in any country affected and make information available to the GFIU.

357. **Criterion 35.2** – The sanctions provided by the 2019 Sanctions Act (Part II par.7(1, 4), Part II par.9(1,2) and Part V par.51(1, 2)) are applicable both for corporate bodies and their directors, managers, secretaries or other similar officer or person who was purporting to act in any such capacity.

358. In the case of the criminal offences provided by POCA, S.34 explicitly provides for the applicability of the sanctions to any director, manager, secretary or other similar officer of the body corporate or any other person who was purporting to act in any such capacity.

359. In addition, Reg.20 of the SBPR Act provides for administrative sanctions, such as banning a person from exercising managerial functions in a RFB, if that person is responsible for a default or breach of a relevant person's obligations under the Act or any applicable law or guidance.

Weighting and Conclusion

360. There are few instances where certain requirements, created solely by the AMLGN, are not enforceable. **R.35 is rated LC.**

Recommendation 36 – International instruments

361. In the 2007 IMF assessment report Gibraltar was rated PC with former R.35 and SRI, mainly due to the lack of implementation of the Vienna Convention. Additionally, the International Convention for the Suppression of the Financing of Terrorism (ICSFT) was not extended to Gibraltar at the time. Nevertheless, certain provisions of both conventions were mirrored in domestic acts.

362. **Criterion 36.1** – Gibraltar implements the provisions of the 1988 Vienna Convention (extended to Gibraltar on 2 July 2014) and the 2000 Palermo Convention (extended to Gibraltar on 27 November 2007). However, the Terrorist Financing Convention and the Merida Convention (UN Convention against Corruption) have not been extended to Gibraltar.

363. **Criterion 36.2** –The Vienna Convention is implemented through the 2011 Crimes Act, the 1986 Import and Exports Act, the 2011 Criminal Procedure and Evidence Act, the 2015 Proceeds of Crime Act, the 1995 Drug Trafficking Offences Act, the 2006 Transnational Organised Crime Act, the 2005 Mutual Legal Assistance (EU) Act, and the 2005 Mutual Legal Assistance (International) Act. Some provisions of the Vienna Convention, notably Article 15, 17 and 19, do not appear to be fully implemented in the national legal order. One reservation was made to the Vienna Convention stating that in certain circumstances the Gibraltar would grant immunity only upon request. This does not impair implementation of the Convention.

364. The 2000 Palermo Convention (UN Convention against Transnational Organised Crime) is implemented primarily through the 2006 Transnational Organised Crime Act.

365. The Terrorist Financing Convention (the International Convention for the Suppression of Financing of Terrorism) has not been extended to Gibraltar. However, its provisions have been largely implemented into domestic law through the 2018 Terrorism Act, the Terrorist Asset Freezing Regulations, the 2015 Proceeds of Crime Act, the 2018 Extradition Act, the 2011 Crimes Act, the Consular Relations Act and other legislation.

366. Similarly, the Merida Convention has not been extended to Gibraltar, even though Gibraltar has implemented a significant part of the Convention's provisions to its national legislation – the 2015 Proceeds of Crime Act, The 2011 Crimes Act, the 2018 Extradition Act, the 2006 Transnational Organised Crime Act, the 2005 Mutual Legal Assistance (EU) Act, and the 2005 Mutual Legal Assistance (International) Act.

Weighting and Conclusion

367. Gibraltar is party to the relevant treaties with the exception of the International Convention for the Suppression of Financing of Terrorism and the Merida Convention. Gibraltar has transposed to its domestic legislation to some extent the provisions of the Merida and the FT Convention. **R.36 is rated PC.**

Recommendation 37 - Mutual legal assistance

368. In the 2007 IMF assessment report Gibraltar was rated LC for former R.36 and SR.V. The assessors noted that there was some concern about the ability of Gibraltar authorities to provide assistance, in particular during the investigative stage prior to formal commencement of “proceedings”, which was available only in drug related cases with respect to countries outside the EU.

369. **Criterion 37.1** – Gibraltar has a legal basis based on several acts, that allows its authorities to provide rapidly a wide range of mutual legal assistance in relation to ML, associated predicate offenses and FT investigations, prosecutions and related proceedings, namely:

The 2005 Mutual Legal Assistance (European Union) Act (MLA (EU)),

The 2014 European Freezing and Confiscation Orders Regulations (EFCO Reg.),

The 2017 European Investigation Orders Regulations (EIO Reg.),

The 2005 Mutual Legal Assistance (International) Act (MLA (INT)),

The Transnational Organised Crime Act 2006 (TOCA),

Proceeds of Crime Act 2015 (External Requests and Orders) Order 2019 (ERO Ord)

Proceeds of Crime Act 2015 (External Investigations Ancillary to a Criminal Investigation or Proceedings) Order 2019 (EICIP Ord),

Proceeds of Crime Act 2015 (External Investigations in a Civil Context) Order 2019 (EIC Ord),

The 1995 Drugs Trafficking Offences Act (DTOA),

The 1948 Evidence Act (EA).

370. The range of assistance includes service; obtaining statements and evidence; entry, search and seizure, prisoner transfer; and restraint and confiscation (DTOA and Orders under POCA, namely ERO Ord, EICIP Ord and EIC Ord. The assistance in the Orders can be provided in respect of proceedings or investigations regardless of the existence of a treaty or reciprocity.

371. **Criterion 37.2** – In Gibraltar, the Minister of Justice is responsible for MLA requests and requests under the EFCO Reg. The central authority for assistance requests and requests falling under the European Investigation Order (EIO Reg.) is the Attorney General of Gibraltar. The competent authority for receiving and processing the aforementioned requests is the Attorney General. A spreadsheet of the requests is maintained, and actions are diarised and monitored. Requests under Part III of the MLA(EU) do not go through the Attorney General, but direct to the Commissioner of Income Tax and are therefore not taken into account in the case management system of the AG but in a separate management system.

372. An assessment of the urgency of the request takes place on receipt of the same and requests are prioritised in accordance with established policy on prioritisation. Both the Attorney General and the RGP have developed a process for the timely prioritisation and execution of

requests. When a request/ EIO is processed, consideration is given to the urgency stated for prioritisation, on the basis of circumstances such as: the person being investigated is in custody, there are fixed trial dates, evidence is at risk of being lost/ dissipated, co-ordinated actions required, etc. Requests involving FT are automatically prioritised. EIOs are recognised within 30 days and must be executed within a further 90 days (regulation 16).

373. **Criterion 37.3** – Gibraltar has no unduly restrictive or unreasonable conditions in place for the provision of MLA under the MLA (EU), MLA (INT) and DTOA. In order to proceed with requests according to the MLA (INT) either an agreement has to be signed (1 existing) or reciprocity has to be declared by the requesting country. Under the MLA (EU) and the MLA (INT) it is not possible to compel a servant of the Crown to give evidence (no such restrictions under the DTOA and the EIO Regulations). There are also provisions allowing the delay of forwarding any property or evidence under the MLA (EU) if the evidence is required in connection with pending criminal proceedings in Gibraltar. The EIO Regulations outline grounds for refusing to recognise or execute an EIO, in accordance with the relevant EU directive. The Evidence Act is restricted in enabling assistance once proceedings have commenced (it does not apply at the investigative stage). A person cannot be compelled to give evidence, where in doing so he/she would prejudice the security of Gibraltar - MLA (EU) and MLA (INT) and section 11 of the EA. The request for assistance can be refused in the case when criminal proceedings associated with the request are identified as having a political character (section 12 EA). Dual criminality is required in certain circumstances (see criterion 37.6).

374. Gibraltar authorities have indicated that if coercive measures are sought to be carried out and the statutory requirements of one act are not met, this would be carried out by a different act if possible or on a voluntary basis. If it is acceptable by the requesting state, requests for assistance and EIOs can be sent directly to the competent authority in Gibraltar and not through the Foreign Commonwealth Office in London.

375. **Criterion 37.4** –

a) The MLA(INT) contains a broad exclusion of fiscal offenses from the definition of “offense”. However, authorities have indicated that if the underlying conduct of the offences constitutes an offence in Gibraltar such as fraud, conspiracy to defraud or false accounting, ML etc, the request would be actionable. Similarly, under the MLA (EU) assistance does not cover fiscal offences other than offences relating to excise duty, value added tax or customs duties. However, assistance may be refused when the request relates to excise duties, value added tax or customs duties and the alleged amount of duty underpaid or evaded does not exceed EUR 25,000 or where the presumed value of the goods exported or imported without authorisation does not exceed EUR 100,000, unless, given the circumstances or identity of the accused the case is deemed to be extremely serious by the requesting State (MLA EU and INT Act). In both Acts, it is the underlying conduct which is important, and a request will be actioned if the same amounts to an offence. Authorities have indicated that between 2016 and 2018, there have been no requests denied on the basis of the fact that the request concerns a fiscal offence.

b) Secrecy or confidentiality does not constitute a ground for denying a request, where information is kept on an implied or express undertaking of confidence, the Central Authority can nominate a court to recover evidence or direct that a search warrant or production order to be applied (section 12, 13 & 15 of the MLA (EU) and MLA (INT) and Part 2 of the CP&EA), with the exception of legally privileged material.

376. **Criterion 37.5** – Requests for legal assistance are treated confidentially, although no specific provisions regulate this aspect. Entities or witnesses from whom evidence is required are not provided with a copy of the MLA request and they are only informed of the necessary details to

enable them to provide the evidence requested. Witnesses could be charged for tipping off or for perverting the course of justice should they disclose the fact that there is an investigation, or an investigation is being contemplated in connection with any offence. Also, the 2012 MLA (International Rules) and the 2012 MLA (European Union) Rules provide the public to be excluded from proceedings if necessary. In addition, all government employees and law enforcement are required to sign the Official Secrets Act when they are employed and retain a duty of confidentiality.

377. **Criterion 37.6** – In General, dual criminality is not a feature of either MLA (EU) or MLA (INT) in order to receive evidence or assistance which does not involve coercive actions. However, in the case where assistance is provided under the TOCA via the MLA (INT), there is an element of dual criminality as TOCA requires an offence to be relevant i.e. an offence which is punishable in Gibraltar by imprisonment for a period of 4 years or more (and the country is party to the UNTOC). Nevertheless, if a declaration of reciprocity is included in the request or subsequently provided, it would be possible to process the request under the MLA (INT) instead of accessing the act via TOCA.

378. **Criterion 37.7** – Dual criminality is required in the MLA (EU) and MLA (INT) for the purpose of search and production orders. In respect of search, there is a requirement that the underlying conduct constituting the alleged offence must also constitute an offence in Gibraltar and would, if it had occurred in Gibraltar, be punishable by imprisonment for a period of at least 6 months. In respect of a production order, it will be granted where the offence, had it been committed in Gibraltar, would have constituted an indictable offence or an offence which is included in Schedule 14 of the Criminal Procedure & Evidence Act (CP&EA). As indicated in criterion 37.6, the TOCA requires the request to concern a relevant offence. Section 44 of the DTOA also indicates, that the enforcement of overseas forfeiture orders under the act applies to an offence which corresponds to a drug trafficking offence or to an offence under the Drugs (Misuse) Act.

379. Gibraltar takes a conduct-based approach to assessing dual criminality. Technical differences between the offence's categorisation do not prevent the provision of assistance, providing that the underlying conduct is criminalised in both jurisdictions.

380. **Criterion 37.8** – Requests for assistance to the competent authorities must be made in order to be able to obtain the information for evidential purposes. Otherwise, information can be provided on an intelligence basis only. As indicated in C.37.7 the MLA(EU), the MLA(INT) and the DTOA provide for the execution of search warrants, production orders for the search, seizure of information, documents or evidence on the basis of a request for assistance, taking also into account the conditions set out in criteria 37.3 & 37.4. The EA can also be used for obtaining evidence only once proceedings have commenced. Apart from using coercive measures, it is also possible to obtain witness statements, if the witnesses are willing to provide them voluntarily. The EIO Regulations allow for any assistance/investigative measures that are available domestically to be also used to respond to requests for assistance. Cooperation with Ireland and Denmark is regulated more thoroughly under the MLA (EU) and EFCO Reg. Controlled delivery can only be used in the context of requests for assistance filed under the TOCA. As indicated in R.31, intercepting communications by LEAs is currently not permitted in Gibraltar.

Weighting and Conclusion

381. All criteria are met. **R.37 is rated C.**

Recommendation 38 – Mutual legal assistance: freezing and confiscation

382. In the 2007 IMF Report, Gibraltar was rated partially compliant in respect of these requirements. The MLA provided by Gibraltar authorities was limited by significant impediments in its legal framework: 1) there was no power in respect of the following: (except in drug-related cases) to secure restraint or charging orders in respect of criminal property where proceedings were pending; to seize suspected criminal property at the border 2) there was no promulgation of an order provided for in the CJO listing countries by which non-drug related confiscation orders might be registered and enforced in Gibraltar.

383. **Criterion 38.1 (Met)** – Gibraltar has the ability to respond to foreign requests to identify, freeze, seize and confiscate property.

(a) Laundered property can be identified on behalf of a state through search and seizure, production orders, disclosure orders, customer information orders and account monitoring orders provided there is an investigation in the requesting state into whether the property was illegally obtained, the whereabouts of illegally obtained property, or ML (section 184D POCA; sections 6, 13, 16, 22, 29 POCA (External Investigations Ancillary to a Criminal Investigation or Proceeding) Order 2019). This property can be seized or restrained where there is an on-going investigation or proceedings in the requesting state, or the requesting state has obtained a corresponding foreign order (section 6 POCA (External Requests and Orders) Order 2019). Confiscation orders can be obtained on the basis of an equivalent order from a requesting state (section 18 POCA (External Requests Orders) Order 2019).

(b) Proceeds can be identified, seized and restrained on behalf of a requesting states using the mechanisms described above at criterion 38.1(a).

(c) and (d) instrumentalities used or intended for use in ML, FT or predicate offences can be identified, seized and restrained on behalf of a requesting states using the mechanisms described above at criterion 38.1(a).

(e) property of a corresponding value can be identified, seized and restrained on behalf of a requesting states using the mechanisms described above at criterion 38.1(a).

384. **Criterion 38.2** – Gibraltar is capable of providing assistance in the context of non-conviction-based confiscation and related proceedings, including in circumstances where a perpetrator is unavailable by reason of death, flight, absence, or where the perpetrator is unknown. Instrumentalities, proceeds and laundered property can be identified through a range of available investigative measures which can be exercised on behalf of another state (sections 6, 13, 16, 22, 29, 40 of POCA (External Investigations in a Civil Context) Order 2019). The Supreme Court can also issue an order to freeze or confiscate this property, or property of a corresponding value, where there is an on-going investigation or proceeding in the requesting state, or where a corresponding foreign order has been issued, provided there is dual criminality (sections 31, 33 POCA (External Requests and orders) Order 2019).

385. **Criterion 38.3** – a) The Joint Investigation Teams Regulations 2014 make provision for the setting up of joint investigation teams with EU MSs and regulate the purpose, conditions and use of information obtained. In respect of non-EU MSs, arrangements can be made on a case by case basis for investigation and coordination of actions, although any information obtained, if required for evidential purposes would need to be requested through MLA.

386. Gibraltar has the mechanisms to manage and dispose of property, seized or confiscated on behalf of foreign states, including the appointment of receivers and management receivers.

387. The Cooperation between Asset Recovery Offices Regulations 2014 transposes the Council Decision 2007/845/JHA concerning cooperation between Asset Recovery Offices of the Member States. As already noted under R.4, the Asset Recovery Office within the RGP would be responsible for the managing and where necessary, the disposal of frozen, seized or confiscated assets. With regard to non-EU MS, Gibraltar has mechanisms to manage and dispose of property frozen, seized or confiscated on behalf of a foreign state, including the appointment of receivers (or enforcement receivers by virtue of POCA (External Request and Orders) Order 2019. The said Order and the other Orders made under sections 184A to D apply to external requests and orders from any external state. In the event of a foreign conviction and a request for confiscation in Gibraltar, chapter 2 of POCA (External Request and Orders) Order 2019, article 41 provides for the appointment of enforcement receivers. In civil recovery proceedings where there has been a request for MLA, a property freezing order may be made. As indicated above at criterion 38.2, article 72 of POCA (External Request and Orders) Order 2019 allows for the Attorney General to apply to the Supreme Court for a property freezing order in civil recovery proceedings. The Supreme Court may appoint a receiver in respect of any property to which the property freezing order applies. The powers of the said receiver are set out in article 77 and paragraph 5 of Schedule 1 and include management powers and anything that is reasonably required to manage/preserve the property.

388. **Criterion 38.4** – Regulation 25(5) of the EFCO Reg. in connection with EU Member States, specify that where the amount obtained in relation to an overseas confiscation order is greater than or equal to an amount equivalent to 10,000 Euros, the Supreme Court must order the transfer of 50% of the amount obtained, unless otherwise agreed between the Central Authority in Gibraltar and the court of authority in the Requesting State. Whilst no formal mechanism is available for countries outside EU, the authorities advised that it would be possible to enter into ad hoc asset sharing agreements. Any such agreement would need to be approved by the court.

Weighting and Conclusion

389. All criteria are met. **R.38 is rated C.**

Recommendation 39 – Extradition

390. In the 2007 IMF Report, Gibraltar was rated partially compliant with the former R.39 and largely compliant with SR.V. The authorities had not elaborated specific procedures for processing requests. Gibraltar could not be given a fully compliant rating under the previous FATF methodology without specific experience of dealing with a FT extradition request.

391. **Criterion 39.1** –

a) ML and FT are extraditable offences in Gibraltar. The extradition regime in Gibraltar is governed by three pieces of legislation. The extradition regime in Gibraltar is governed by several pieces of legislation: the European arrest warrant Act (EAWA) 2004 which also applies to the UK gives effect to the Council Framework Decision of the 13th June 2002 on the European arrest warrant and the surrender procedures between EU member states; the Extradition Act 2018; the Fugitive Offenders Act (FOA) 2002; and the Terrorism Act 2018 which enables the extradition of any person from Gibraltar under any provision of law on extradition for any terrorist offence under sections 134 to 139.

392. There is a case management system and clear processes for the timely execution of requests including prioritisation where appropriate. Few extradition requests are received, any request received is given a high priority.

b) Gibraltar does not place any unreasonable or unduly restrictive conditions upon the execution of requests.

393. Under the EAWA, in accordance with the Framework Decision, extradition will be denied where the surrender would be contrary to the Convention for the Protection of Human Rights and Fundamental Freedoms or the Gibraltar Constitution; the request was made for the purpose of prosecution or prejudice on account of race, religion, nationality, language, gender, sexual orientation or political opinion; the person could be sentenced to death or would be subjected to torture or inhuman or degrading treatments (section 26); the person has been granted a pardon or is immune (section 28); the expiration of time (section 29); double jeopardy (section 30).

394. Under the Extradition Act 2018, extradition would only be prohibited: if the person could face the death penalty (section 30); double jeopardy (section 18); if the request as on account of a person's race, religion, nationality, gender, sexual orientation or political opinion or if their trial would be prejudiced as a result of the former (section 19); the passage of time (section 20); hostage-taking considerations (section 21); if there are no specialty arrangements with the requesting state (section 31 – but this does not apply where the person consents to their extradition) and where the person has previously been extradited to Gibraltar from another state and consent has not been given for the further extradition (section 32).

395. Under the FOA, the only restrictions on return are where an offence is of a political character; if the offence is motivated on account of a person's race, religion, nationality or political opinions or that the person's liberty is at risk on account of the former (section 5).

396. **Criterion 39.2** – There is nothing in the EAWA, Extradition Act 2018 nor in the FOA which prevents the extradition of Gibraltar's own nationals. There is however, a requirement that the issuing State provide a guarantee that where the EAW relates to a Gibraltar national of a resident, they must, after being surrendered and after being heard, be returned to Gibraltar to serve the custodial sentence or detention order (section 8A (3) EAWA).

397. **Criterion 39.3** – The dual criminality requirement is deemed to have been met as long as underlying criminal conduct is an offence in Gibraltar. Gibraltar takes a conduct-based approach to assess the dual criminality; technical differences between the offence's categorisation do not prevent extradition provided that the underlying conduct is criminalised.

398. **Criterion 39.4** – The Extradition Act 2018 also allows for the direct transmission of extradition requests. Section 6 provides for transmission to the Central Authority and also allows for copies to be transmitted by fax or email to the Central Authority or to the Magistrates' Court.

399. Under the Extradition Act 2018, a person can also consent to their extradition under sections 63 and 64. Where a person consents to be surrendered, the Magistrate must send their case to the Central Authority for the Central Authority's decision to extradite the person who will decide to do so unless he is prohibited from doing so (section 30, death penalty and section 32, an earlier extradition to Gibraltar from another requesting state and consent has not been granted). The person must be extradited within two months of the Magistrate sending the case to the Central Authority.

400. Under the FOA requests can also be sent directly to the Governor.

401. The EAWA provides a simplified extradition mechanism for EAW requests from EU member states and the United Kingdom.

402. The EAWA allows for the direct transmission of EAW requests to Gibraltar. Section 8 provides that an EAW shall be transmitted by or on behalf of the issuing judicial authority to the

Central Authority in Gibraltar or if the location of the person is known, direct to the Magistrates' Court. The transmission requirement is deemed to be satisfied if a copy of the EAW is transmitted by the issuing judicial authority to the Central Authority in Gibraltar by fax or email.

403. Under the EAWA, a person may consent to their extradition under section 11. A person who consents must be surrendered within 10 days of the order of surrender being made, unless a later date is agreed between the issuing and executing authorities.

Weighting and Conclusion

404. All criteria are met. **R.39 is rated C.**

Recommendation 40 – Other forms of international cooperation

405. In the 2007 IMF assessment report Gibraltar was rated compliant with the requirements of R.40.

406. **Criterion 40.1** – Gibraltar competent authorities, have broad powers to provide the widest range of international cooperation at operational level in circumstances where MLA procedures are not required. Timeframe vary between different authorities, but there are no legal impediments preventing a rapid response. Exchanges of information can be conducted both spontaneously and upon request.

407. **Criterion 40.2** –

- a) Authorities have indicated several acts as a legal basis for exchanging information, namely:
- The Cooperation between Asset Recovery Offices Regulations 2014,
 - The Exchange of Information and Intelligence between European Law Enforcement Authorities Regulations 2014,
 - The Joint Investigation Teams Regulations 2014,
 - The Proceeds of Crime Act 2015,
 - The Imports and Exports Act 1986,
 - Supervisory Bodies Regulations 2017,
 - The Gambling Act 2005,
 - Data Protection Act 2004,
 - The Financial Services (Information Gathering & Cooperation) Act.
- With the exception of the FS(IG&C) A, the Gambling Act and the Data Protection Act, these regulations refer to cooperation with EU/EEA states. There is no legal framework for police-to-police cooperation outside of the above legislation, although this is carried out through intelligence channels such as the CARIN (Camden Asset Recovery Interagency Network), Interpol or direct contact.
- b) The GFIU also refers to the Egmont Group agreements. Data held by a third party, created during the course of business and held in confidence is known as a special procedure material. The RGP requires a judicial order to oblige the holder to supply this data. Therefore, obtaining such information may at times require a MLA or EIO. Though this can be overcome if the information supplied causes a local investigation to commence, data is obtained for the local investigation and shared on an intelligence basis with the requesting country.
- c) Competent authorities have appropriate mechanisms or channels for secure transmission and execution of requests. For example, the GFIU uses the Egmont Secure Web (ESW) to communicate with foreign FIUs in a secure manner. Interpol secure network is used by the GCID. HMC uses its liaison officers in London, Madrid and Malaga, and the Mar/Yacht-Info SOUTH network. As regards the GGC, centralised points of contacts have been established with its foreign

counterparts. Also, information is exchanged during the working groups of the Gaming Regulators European Forum and the International Association of Gaming Regulators. The GFSC cooperates with foreign counterparts through IOSCO, SIS, GIFICS and FIN.net channels

d) Competent authorities have in place processes for prioritisation of incoming requests and their timely execution. For example, the RGP has SOP's for the prioritisation of urgent requests. The Head of GFIU prioritises the execution of requests. Some authorities have indicated, that due to the low number of incoming requests, all are initiated upon receipt.

e) Competent authorities are bound by data protection laws, such as the Data Protection Act and the Official Secrets Act and the GDPR. Nevertheless, only the GFIU, RGP, HMC and GFSC have indicated procedures to safeguard received data.

408. **Criterion 40.3** – The GFIU, the GFSC and the GGC do not need a bilateral or multilateral agreement or arrangements to co-operate, but they will sign MoUs where required by the other party and where this is to improve the efficacy of information exchange.

409. **Criterion 40.4** – Competent authorities are able to provide timely feedback upon request to foreign authorities who have provided assistance, although this is not systematic and consistent across agencies. The GFIU has a feedback system for Egmont in place. The Office of Advisory Council (OAC) can also provide feedback regarding MLA and EIO upon request. The GGC can also provide such feedback. The RGP, the GFSC and HMC are able to give feedback to jurisdictions that have supplied it data at their request. HMC also uses liaison officers for this purpose.

410. **Criterion 40.5** – No unreasonable or unduly restrictive conditions on, the provision of exchange of information has been identified. Gibraltar authorities (the GFSC, HMC, RGP and the GFIU) have indicated that the inclusion of fiscal matters is not a potential obstacle for co-operation. When an inquiry is on-going in Gibraltar, consultation with the requesting authority would take place on the use of any information supplied. Gibraltar authorities have indicated, that when the nature or status (civil, administrative, law enforcement, etc.) of the requesting counterpart authority is different from that of its foreign counterpart this does not constitute an obstacle to exchange information.

411. The GFIU does not have any unreasonable or unduly restrictive conditions in sharing information provided that measures are taken into account (e.g. a risk assessment is carried out on the intelligence being provided, ensuring that the country where the information is sent is GDPR compliant or similar, that there are special handling conditions specified such as the use of the information for intelligence purposes only).

412. **Criterion 40.6** – The GFIU under Sec 11 A(2) of POCA, ensures that information received from an FIU is used only for the purpose and by authorities for which information was sought or provided unless prior authority is given by the requested competent authority. In most cases this will be done by applying special handling conditions on an intelligence report. As an Egmont member, the GFIU applies the Data Protection and Confidentiality of Egmont's Principles of Information Exchange.

413. The GFSC under the Financial Services (Information Gathering and Co-Operation) Act 2013 (s.4) shall not transmit information to other bodies or persons without the express agreement of the authority which disclosed it and shall use the information solely for the purposes for which those authorities give their agreement, except in duly justified circumstances, in which case the Authority shall immediately inform the authority that sent the information.

414. In line with the Exchange of Information and Intelligence between European Law Enforcement Authorities Regulations 2014, information received by the RGP from other

jurisdictions will only be used for the purpose it was obtained which would be detailed at the time of the request.

415. **Criterion 40.7** – Gibraltar authorities are obliged to ensure a level of confidentiality appropriate to any request for co-operation and the information exchanged, in accordance with relevant data protection legislation. No distinction with regard to the level of protection of information from foreign authorities and domestic sources was identified. FIU information/intelligence supplied to other FIUs or LEAs whether local or foreign is sanitised and sent through a 3x5x2 intelligence report with a caveat that information/ intelligence provided shall only be used for intelligence purposes and it is not to be disseminated without the prior permission by the GFIU. In line with the DPA 2004, competent authorities cannot provide information to third countries without verifying that appropriate safeguards exist to protect the data requested. Under Sec 1I (5)(e) of POCA, the GFIU can refuse a request for information where disclosure of that information would not be in accordance with the fundamental principles of Gibraltar law (DPA 2004).

416. Under the scope of the FS(IG&C)A the GFSC may refuse to provide information if it is not satisfied that the recipient is subject to equivalent confidentiality provisions (S4(5)). Similarly, the Gambling Act (S.6(6)(f)) allows the GGC to refuse to provide information where it is deemed that the requesting competent authority will not be able to adequately safeguard that information.

417. **Criterion 40.8** – Competent authorities in Gibraltar (in particular the HMC, RGP, GFIU, GCID) are able to conduct inquiries on behalf of foreign counterparts, and exchange with their foreign counterparts almost all information. Competent authorities (apart from the GFSC, GGC and GFIU) mostly base their power to do so on legal acts concerning cooperation with EU/EEA States. Intrusive enquiries conducted by the RGP and HMC, such as production orders and search warrants will be conducted if there is a local investigation. If the grounds disclosed within the request for information give rise to a reasoned suspicion of offences in Gibraltar, a local investigation may be commenced. The data obtained as part of that investigation may then be transmitted for intelligence to the requesting state on an intelligence basis. As requests relate to financial products of asset tracing there will be the ability to conduct a local investigation and provide all information to foreign counterparts. The GFIU conducts inquiries on behalf of foreign counterparts. The GGC may conduct enquiries on behalf of foreign counterparts and exchange information with them on the same basis as if inquiries were being carried out domestically.

418. The FS(IG&C) A permits the GFSC to disclose information to any third party that meets the criteria. Section 12(2) of IF(IG&C) A permits an officer or agent of a requesting authority to exercise the powers conferred to national authorities' representatives, upon a previously communicated request from the foreign authority.

419. **Criterion 40.9** – Section 1C(c) of the POCA provides that one of the main functions of the GFIU is to exchange information regarding criminal conduct with FIUs and other similar bodies and LEAs within and outside of Gibraltar. In accordance with section 1E (1) the GFIU shall exchange with other FIUs and Egmont Group FIUs, spontaneously or upon request, any information that may be relevant for the processing or analysis of information related to ML/FT.

420. **Criterion 40.10** – The GFIU generally provides feedback to foreign counterparts on request and where possible, it may provide spontaneous feedback on the use of information.

421. **Criterion 40.11** – The GFIU is able to exchange:

a) information with other FIUs and Egmont Group FIUs, spontaneously or upon request, any information that may be relevant for the processing or analysis of information related to ML/FT (Section 1E(1) of the POCA). The GFIU has access (directly or indirectly) to most domestic LEA

databases. In the case where access is not available due to technical issues, the GFIU can obtain information upon a written request.

b) other information which it can obtain or access through the whole range of its available powers which it would normally use domestically for receiving and analysing information and must respond to any such request in a timely manner (section 1F(1), 1GA(1) of the POCA).

422. **Criterion 40.12** – The GFSC can provide to an authority of Gibraltar (a list of authorities is provided in the FS(IG&C)A) or to a similar supervisory authority outside of Gibraltar, any information received under the Financial Services Act ((FS(IG&C)A) section 4(1)). The powers of GFSC include the possibility to compel any documents from relevant persons and to make enquiries. Section 3 deals with data protection rules consistent with EU Regulations. However, disclosure of information is not limited by data protection rules, as long as it is provided to another authority in Gibraltar or to a similar foreign counterpart.

423. **Criterion 40.13** – The GFSC has the power to obtain information from regulated firms for the purpose of assisting its foreign counterparts (FS(IG&C)A section 12). Also, the GFSC has the authority to require a relevant person to attend before GFSC and provide any information requested or document that is “*reasonably required*” (FS(IG&C)A) section 6(1)).

424. **Criterion 40.14** – The GFSC can exchange any information it holds (including regulatory information, prudential information, and AML/CFT information) with other supervisors. The FS(IG&C)A (section 12) provides for disclosing information with the purpose of assisting an authority which exercises supervisory or regulatory responsibility over a relevant person (any firm or person involved with the firm), or any part of a group which a firm belongs to. There seems to be no other restriction except for GFSC to consider if the disclosure is for purpose of assisting another authority.

425. **Criterion 40.15** – Section 12(2) of IF(IG&C)A permits an officer or agent of a requesting authority to exercise the powers conferred to national authorities’ representatives, upon a previously communicated request from the foreign authority. Furthermore, the GFSC is able to exercise domestic powers and conduct inquiries on behalf of overseas regulators (Section 12(1) of the FS(IG&C)A). There are a number of reasons to deny such as breach of Gibraltar’s laws; double jeopardy; the request is not made in accordance with the provisions of a MoU; and on grounds of public interest or essential national interest (section 13 of the FS(IG&C)A).

426. **Criterion 40.16** – The GFSC acts in accordance with the IOSCO MMOU which requires supervisors to use the information solely for the purposes specified as part of the request for information, unless prior consent is obtained from the requested authority.

427. According to the FS(IG&C)A (section 4(3c, c)) the GFSC shall not transmit such information to other bodies or persons without the express agreement of the authority which disclosed it; and it shall use the information solely for the purposes for which those authorities give their agreement, except in duly justified circumstances, in which case the GFSC shall immediately inform the authority that sent the information.

428. **Criterion 40.17**– LEAs in Gibraltar are able to exchange all domestically available information with their foreign counterparts. Nevertheless, for information where a judicial order is required (e.g. banking data), this would require a MLA request or an EIO. Data held by a third party, created during the course of business and held in confidence is known as a special procedure material. LEA’s require a judicial order to oblige the holder to supply such data. There is no impediment to the sharing of this data by LEA’s once it is obtained by legal means. Other authorities have not indicated any limitations related to this aspect.

429. **Criterion 40.18** – LEA’s are able to conduct inquiries and use domestically available, non-coercive powers and investigative techniques to conduct inquiries and obtain information on behalf of foreign counterparts through the use of data requests under the Data Protection Act.. Where coercive information is required, Gibraltar LEA’s can open an investigation (if there is a Gibraltar nexus) or a formal MLA request can be made.

430. Requests conducted under the EIO Regulations allow all domestically available investigative methods to be used by LEA’s. Police co-operation takes place particularly within the framework of agreements signed by Interpol (Cooperation between RGP and GCID). Cooperation is also conducted via, CARIN, AMON, liaison officers and other police-to-police requests. Gibraltar is not a member of Europol or Eurojust at present, so this pathway is not available for the exchange of information.

431. **Criterion 40.19** – In line with section 3 of the 2014 Joint Investigation Teams Regulations (JIT Regs), by mutual agreement with the competent authorities of at least one EU Member State, the Commissioner of the RGP may set up a joint investigation team. The joint investigation team shall be set up in Gibraltar or in one of the Member States in which the investigations are expected to be carried out. According to section 12 of the JIT Regs, persons other than representatives of the competent authorities of the Member States setting up joint investigation teams may be authorised to take part in the activities of the team (e.g. the HMC). Gibraltar authorities indicate a bilateral or multilateral arrangement is not required to enable joint investigations but can be entered into if required by other jurisdictions. There is no legislation with regard to forming a JIT with non-EU states, but in the case of the RGP, a MoU could be arranged to provide for such cooperation. Nevertheless, the obtaining of evidence in this situation would be governed by the DPA and MLA legislation.

432. Though there is no legislation for the setting up of a local JIT between Gibraltar authorities this can and has been done through the signing of MoU’s between authorities. This has occurred previously in Gibraltar and a local JIT is currently in place for a ML investigation.

433. **Criterion 40.20** – The GFIU can exchange information regarding criminal conduct with foreign non-counterparts (law enforcement agencies outside Gibraltar under Sec 1C(1)(c)). When doing so, it provides the necessary background information to allow its counterparts to make a clear distinction between co-operation sought for intelligence purposes and information requested for purely investigative purposes. In the case of the GGC section 6 of the Gambling Act provides broadly for exchanging information with counterparts and non-counterparts.

434. LEA’s such as HMC and RGP can directly and indirectly exchange information with non-counterparts (e.g. the RGP’s exchanges with the Insolvency Service in the UK). This is also the case with the GFSC.

435. Apart from the GFIU, there is no obligation to provide information on whether competent authorities’ indirect requests always make clear the reasoning and on whose behalf the request is made. Nonetheless, this has been indicated by authorities as common practice, subject to counterpart not objecting to it.

Weighting and Conclusion

436. Gibraltar’s framework for international co-operation is comprehensive, and includes the majority of required elements, though some minor gaps remain. **R.40 is rated LC.**

Summary of Technical Compliance – Key Deficiencies

Compliance with FATF Recommendations

Recommendations	Rating	Factor(s) underlying the rating
1. Assessing risks & applying a risk-based approach	PC	<ul style="list-style-type: none"> Gibraltar did not properly identify all of its ML/FT risks. The analysis of the threat, particularly cross border, and of the vulnerabilities is not comprehensive; Exemptions from the application of the FATF Standards and the application of simplified and enhanced CDD requirements are not based on verified risks; Information on higher risks identified by the country is not explicitly requested to be incorporated in the firms' risk assessments; Simplified due diligence is allowed when the financial business identifies areas of lower risk – however, it is left to the discretion of financial businesses to determine when and based on their' assessment of risk, which does not necessarily need to take into account information on risks identified at national level; No specific provision prohibiting simplified due diligence whenever there is a suspicion of ML; Except for TCSP, the other DNFBPs are not required to monitor implementation of their risk management systems and enhance them if necessary; No measures for the new risks identified in the 2018 NRA and no risk-based allocation of resources for the supervision of lawyers and notaries (although they feature among the highest risks identified by the 2018NRA).
2. National cooperation and coordination	LC	<ul style="list-style-type: none"> The 2017 strategy has not been revised in light of new risks identified in the 2018 NRAs.
3. Money laundering offences	C	
4. Confiscation and provisional measures	LC	<ul style="list-style-type: none"> Not all special investigative means are available for purposes of confiscation.
5. Terrorist financing offence	C	
6. Targeted financial sanctions related to terrorism & TF	LC	<ul style="list-style-type: none"> The requirement to freeze assets that are jointly owned is not expressly stated in the legislation.
7. Targeted financial sanctions related to proliferation	LC	<ul style="list-style-type: none"> The requirement to freeze assets that are jointly owned is not expressly stated in the legislation; No provision specifically requires supervisors to monitor and ensure compliance by FIs and DNFBPs
8. Non-profit organisations	LC	<ul style="list-style-type: none"> There is no specific policy document on the promotion of transparency; There is no outreach or educational programmes to donors have been conducted; No NPOs were involved in the development and refinement of best practices to address FT risk and vulnerabilities; The effective co-operation, co-ordination among all levels of appropriate authorities or organisations that hold relevant information on NPOs is not guaranteed.
9. Financial institution	C	

Recommendations	Rating	Factor(s) underlying the rating
secrecy laws		
10. Customer due diligence	LC	<ul style="list-style-type: none"> • Exceptions to identification and verification requirements are not based on a proven low risk assessment (C.10.3). • There is no explicit requirement to undertake reviews of existing records to ensure that documents, data or information collected under CDD process is kept up-to date and relevant (C.10.7). • There is no explicit provision relating to understanding the nature of the business (C.10.8). • The legal requirement to verify the identity of the customer does not include for legal arrangements the obligation to obtain the name of the relevant persons having a senior management position (C.10.9). • The requirements of identification of the BO do not follow the hierarchy of provisions of identifying the BO in the standards (C.10.10). • In case of trusts, only beneficiaries that hold more than 25% of the property are required to be identified (and not on all beneficiaries) (C.10.11). • There is no explicit provision for the beneficiary of a life insurance product to be considered as a risk factor when determining whether EDD are applicable (C.10.3). • There is no explicit requirement to consider the materiality when applying CDD requirements (10.16). • Guidance on lower risks in relation to EU members is not based on an assessment of risk (C.10.17). • There are no explicit provisions that prohibit the opening of accounts for which CDD has not been performed (C.10.18). • There is no explicit permission not to permit pursuing the CDD process if it is believed this might tip-off the customer (C.10.20).
11. Record keeping	PC	<ul style="list-style-type: none"> • Not all types of transactions are covered by record-keeping requirements in POCA and this shortcoming is only broadly covered by accounting regulations. • The records that need to be kept relate only to the customer's identity and are not explicit on other CDD information (C.11.2). • RFBs must keep supporting evidence and records of transactions (original documents or copies) necessary to identify transactions, rather than to allow transactions to be reconstructed (C.11.3). This provision is covered only through enforceable means and not in law. • Obligation to maintain records so that an enquiry or court order from the authorities can be responded to swiftly, which includes all CDD information and transaction records, is not set out in law (C.11.3) • There is no direct requirement to keep records on account files, but only accounts details when those are used for payments, and this is also not set in law (C11.2).
12. Politically exposed persons	PC	<ul style="list-style-type: none"> • Determining whether a client is a PEP is not mandatory for all customers but can be interpreted as based on a risk sensitive approach (C.12.1(a)). • There is no specific provision for obtaining senior management approval if the BO of the customer is a PEP (C.12.1(b)). • The requirement to establish the source of wealth and source of funds does not cover customers already on-boarded at the time of the adoption of POCA (C.12.1(c)). • The obligation to have policies and procedures to determine if a customer/BO is a PEP does not extend to family members or persons known to be close associates of PEPs (C.12.3).

Recommendations	Rating	Factor(s) underlying the rating
13. Correspondent banking	PC	<ul style="list-style-type: none"> While most criteria are met, they apply only to non-EEA countries and territories, which is not in line with FATF Standards (all criteria).
14. Money or value transfer services	LC	<ul style="list-style-type: none"> There is no explicit requirement for MVTS to include agents in their AML/CFT programs or monitor them (C.14.5).
15. New technologies	C	
16. Wire transfers	C	
17. Reliance on third parties	LC	<ul style="list-style-type: none"> Regarding the timing, information and documentation must be made available by the third party “as soon as reasonably practicable” rather than immediately and without delay (C.17.1(b)). Ultimate responsibility of the functions carried out by the third party remains with the RFB. Nevertheless, RFBs are permitted to rely on third parties by simply having “reasonable grounds to believe” that the third party is regulated and supervised accordingly (C.17.1(c)) Although reliance on third parties established in high risk third countries is not permitted, for all other situations there is no requirement to take into consideration information available on the country risk, apart from membership to the EEA (C.17.2).
18. Internal controls and foreign branches and subsidiaries	LC	<ul style="list-style-type: none"> Some requirements of C18.1 are only applied by FIs ‘where appropriate’ rather than always. In addition, they do not extent to group level (C.18.1 and C18.2). Requirements relating to foreign branches and subsidiaries are largely covered by POCA and AMLGN, but they only apply in case of non EAA states and territories, as there is a presumption in legislation that all EEA countries have similar AML/CFT requirements (C.18.3) FIs are required to inform GFSC and take additional mitigating measures when it cannot apply same standard as in Gibraltar, but this is restricted only to standards relating to CDD, on-going monitoring and record keeping, and not to all AML/CFT measures (C.18.3)
19. Higher-risk countries	LC	<ul style="list-style-type: none"> Nevertheless, some provisions (Criterion 19.2) apply only to non-EEA countries and territories.
20. Reporting of suspicious transaction	C	
21. Tipping-off and confidentiality	C	
22. DNFBPs: Customer due diligence	PC	<ul style="list-style-type: none"> Some deficiencies identified in R.10, 11, 12, 15 and 17, based on provisions of POCA have been covered by sectoral guidelines, such as record keeping for HVDs, REAs and legal professions. However, other new deficiencies arise.
23. DNFBPs: Other measures	LC	<ul style="list-style-type: none"> Deficiencies identified under R18 and R19. have impact on R.23
24. Transparency and beneficial ownership of legal persons	PC	<ul style="list-style-type: none"> The NRA is not specific enough, as it does not analyse the inherent vulnerabilities of the specific types of legal persons that can be created in Gibraltar or their activities; The form for the submission of information to the RUBO contemplates also the option to consider a “relevant legal entity” as an ultimate BO, which is not in line with the FATF definition of BO; There are no sanctions for non-compliance with the requirement to provide the information within 30 days of the change (for corporate or LEs incorporated prior to the commencement of the RUBOR) or with the requirement to provide the information

Recommendations	Rating	Factor(s) underlying the rating
		<p>within 30 days of its incorporation;</p> <ul style="list-style-type: none"> • Whilst corporates and LEs incorporated in Gibraltar are required to obtain and hold adequate, accurate and current information on the BO of the corporate or legal entity, there are no sanctions for non-compliance with this requirement. • There is no requirement for licensed nominee shareholders or directors to maintain information identifying their nominator; • There is no requirement for nominee shareholders and directors to disclose the identity of the nominator to the company or to the register maintained by the CHG; • The CompA provides sanctions for non-compliance with the information filing requirements, but only in the case of late submissions. These sanctions are neither dissuasive nor proportionate.
25. Transparency and beneficial ownership of legal arrangements	PC	<ul style="list-style-type: none"> • The relevant requirement does not apply to express trusts “governed under their law”, as per the FATF definition, but only to a trust (or similar legal arrangement) that “generates tax consequences in Gibraltar”; • Only a corporate or legal entity incorporated in Gibraltar must keep records of the actions taken in order to identify the BOs - this requirement does not apply to trusts; • There is no requirement for trustees of any trust governed under their law to hold basic information on other regulated agents of, and service providers to, the trust, including investment advisors or managers, accountants, and tax advisors; • Professional trustees are subject to the record keeping requirements but, these requirements apply only to customer’s information, and not explicitly BOs; • There are no requirement for trustees to disclose their status to FIs and DNFBNPs; • There are no sanctions in the case of non-professional trustees and in the case of non-compliance with the requirement to provide the information within 30 days of the change (for trusts created prior to the commencement of the RUBOR) or with the requirement to provide the information within 30 days of its incorporation; • Some of the sanctions are not proportionate or dissuasive; • Existence of flee clauses without safeguards to prevent their misuse.
26. Regulation and supervision of financial institutions	PC	<ul style="list-style-type: none"> • The existing legal and regulatory measures are not sufficiently capable to prevent both criminals or their associates from holding or being the beneficial owner of a significant or controlling interest, or holding a management function, in a financial institution as, inter alia, they apply only to new and not to already licensed FIs and they do not extend to beneficial owners of a significant or controlling interest; • The checks on the source of the funds for controller notifiable applicants are not extended to beneficial owners, which is not in line with the Basel Core Principles.
27. Powers of supervisors	C	
28. Regulation and supervision of DNFBNPs	PC	<ul style="list-style-type: none"> • For casinos, existing measures are not sufficiently capable to prevent both criminals and their associates from holding or being the BO of a significant or controlling interest, or holding a management function, in a casino; • There are no legally enforceable or other measures in place to prevent criminals or their associates from being professionally accredited or holding (or being the beneficial owner of) a

Recommendations	Rating	Factor(s) underlying the rating
		<p>significant or controlling interest, or holding a management function, in a DNFBPs (except, but only partially, for REAs and DPMS);</p> <ul style="list-style-type: none"> • External accountants and tax advisors are not subject to systems for monitoring and ensuring compliance with AML/CFT requirements; • Supervision on a risk sensitive basis is not performed for all types of DNFBPs.
29. Financial intelligence units	C	
30. Responsibilities of law enforcement and investigative authorities	C	
31. Powers of law enforcement and investigative authorities	LC	<ul style="list-style-type: none"> • The investigative means of intercepting telephone communications is not regulated by statute and is not permitted by law.
32. Cash couriers	LC	<ul style="list-style-type: none"> • The declaration system applies only to movements (both inward and outward) of cash and BNI from and to the EU; • Penalties for failure to declare cannot be considered proportionate or dissuasive.
33. Statistics	C	
34. Guidance and feedback	C	
35. Sanctions	LC	<ul style="list-style-type: none"> • There are few instances where certain requirements, created solely by the AMLGN, are not enforceable.
36. International instruments	PC	<ul style="list-style-type: none"> • Gibraltar is not a party to the International Convention for the Suppression of Financing of Terrorism and the Merida Convention
37. Mutual legal assistance	C	
38. Mutual legal assistance: freezing and confiscation	C	
39. Extradition	C	
40. Other forms of international cooperation	LC	<ul style="list-style-type: none"> • There is no legal framework for police-to-police cooperation; • Apart from the GFU, there is no obligation to provide information on whether competent authorities' indirect requests always make clear the reasoning and on whose behalf the request is made.

GLOSSARY OF ACRONYMS

AG	Attorney General
AMLGN	Anti-Money Laundering Guidance Notes
AMON	Anti-Money Laundering Operational Network
BCC	Board of Charity Commissioners
BO	Beneficial Owner
BNRA	Business Names Registration Act
B2B	Business to business
CA	Crimes Act
CompA	Companies Act
CFT	Combating the financing of terrorism
CHG	Companies House Registry
CP&EA	Criminal Procedure and Evidence Act
CTR	Cash Transaction Reports
DLT	Distributed Ledger Technology
DPA	Data Protection Act
DTOA	Drug Trafficking Offence Act
EC	European Commission
ECDD	Enhanced Client Due Diligence
EFCO	European Freezing and Confiscation Orders
EIOs	European Investigation Orders
ESW	Egmont Secure Web
ETS	European Treaty Series [since 1.1.2004: CETS = Council of Europe Treaty Series]
EU	European Union
EUSNRA	EU Supra National Risk Assessment
EAWA	European Arrest Warrant Act
FATCA	Foreign Account Tax Compliance Act
FOA	Fugitive Offenders Act
FI	Financial Institution
Fintech	Financial Technology
FT	Financing of terrorism
GACO	Gibraltar Association of Compliance Officers
GBP	British pound sterling
GCID	Gibraltar Coordinating Centre for Criminal Intelligence and Drugs
GD	Gambling Division
GDP	Gross Domestic Product
GFIU	Financial Intelligence Unit
GFSC	Gibraltar Financial Services Commission's
GGC	Gibraltar Gambling Commissioner
GPO	General Prosecutor's Office
HMC	HM Customs
HR	Human Resources
HVDs	High Value Dealers
ICOs	Initial coin offerings
IFC	International Financial Centre

ILOR	International Letter of Request
IMF	International Monetary Fund
INTERPOL	International Police Organisation
IOSCO	International Organisation for Securities Commissions
IT	Information Technology
KRIs	Key Risk Indicators
LEA	Law Enforcement Agency
LoR	Letter of Request
MER	Mutual Evaluation Report
ML	Money Laundering
MLA	Mutual Legal Assistance
NCA	UK National Crime Agency
NCO	National Co-Ordinator for AML/CFT
NRA	National Risk Assessment
OAC	Office of Advisory Council
OCGs	Organised Crime Groups
OCPL	Office of Criminal Prosecutions & Litigation
OFT	Office of Fair Trading
OFSI	Office of Financial Sanctions Implementation (UK)
OPC	Office of Parliamentary Counsel
POCA	Proceeds of Crime Act 2015
PSPs	Payment Service Providers
RBA	Risk-based approach
REAs	Real estate agents
REs	Reporting entities
FRB	Relevant financial business (include FIs)
RGP	Royal Gibraltar Police
RSC	Registrar of the Supreme Court
RUBO	Register of Ultimate Beneficial Ownership
SB	RGP Special Branch
TA	Terrorism Act
TAFR	Terrorist-Asset Freezing Regulations 2011
TOCA	Transnational Organised Crime Act

© MONEYVAL

www.coe.int/MONEYVAL

December 2019

Anti-money laundering and counter-terrorist financing measures

British Overseas Territory of Gibraltar

Fifth Round Mutual Evaluation Report

This report provides a summary of the AML/CFT measures in place in the British Overseas Territory of Gibraltar as at the date of the on-site visit (1 to 12 April 2019). It analyses the level of compliance with the FATF 40 Recommendations and the level of effectiveness of the British Overseas Territory of Gibraltar's AML/CFT system and provides recommendations on how the system could be strengthened.