



**HM Government
of Gibraltar**

**National Coordinator for
Anti-Money Laundering and
Terrorist Financing**

2018 National Risk Assessment

Money Laundering and Terrorist Financing Risks

14 September 2018



1	INTRODUCTION	3
2	METHODOLOGY	4
2.1	EU Supra National Risk Assessment.....	4
2.2	Private and Public sector input	4
2.3	Quantitative v Qualitative Data to support the findings.....	4
3	KEY RISKS	5
4	SUPPORTING DATA ANALYSIS	8
4.1	FIU STR Data	8
4.2	International Information Sharing Data.....	11
4.2.1	Law Enforcement Exchanges.....	11
4.2.2	FIU Exchanges	12
4.2.3	MLA Requests	12
4.2.4	Interpol Requests.....	13
4.2.5	TF	13
4.3	Investigation and Prosecution Data	14
4.4	Financial Services Regulatory Data	16



1 Introduction

This National Risk Assessment (2018NRA) is the second full assessment of Money Laundering (ML) and Terrorist Financing (TF) Risks that face the jurisdiction. The 2018NRA follows on from where the previous iteration left off and builds on the previous version both in terms of scope as well as breadth of the analysis.

In 2016 HM Government of Gibraltar published a ML NRA which was widely distributed amongst the private sector and which had a high level of acceptance with its findings. Public sector authorities undertook a number of risk mitigation actions to reduce the threat and vulnerabilities identified through that process.

In an evolving threat landscape, Gibraltar has to be cognisant of its role in attracting international financial services and products and how these can be attractive to money launderers and terrorist financiers particularly if Gibraltar wants to be at the leading edge of regulatory practices. The good experiences Gibraltar has had in the regulation of the Trust and Company Service Provider (TCSP) sector, Pre-paid Cards, Gambling and now in the Distributed Ledger (DLT) and Initial Coin Offering (ICO) spaces are a testament how good regulatory practices are in themselves effective deterrents to criminal activity without hindering economic development.

The EU recently published a supra-national risk assessment¹ (EUSRNA) covering products and services throughout the EU and how these can be vulnerable to ML and TF risks. As is required by the 4th Money Laundering Directive (4MLD) and our own Proceeds of Crime Act (POCA) we have to factor into our own risk assessment those risks in the context of Gibraltar and existing risk mitigation measures that are in place. It is upon this that the 2018NRA is based upon. Where Gibraltar centric risks have been identified, these have been included in the revision.

By having a full and frank discussion about the potential threats and vulnerabilities that exist within the AML/CFT framework, public sector authorities, judiciary, law enforcement agencies as well as the private sector business can design specific mitigation programmes in strengthen systems of control to deter, prevent and detect possible ML or TF activities.

The presence of a documented risk does not mean that this risk has materialised and is present nor does it mean that there is evidence to support that these ML and TF risks are occurring.

¹ http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=81272



2 Methodology

The previous NRA used a Gibraltar specific risk assessment model based largely on the Financial Action Task Force's own guidance on the formulation of the same. With the publication of the EUSNRA, Gibraltar has forgone its own model and adopted wholesale the EU's methodology for the description of the threats, vulnerabilities and assessment scoring as well as the identification of the relevant risks.

The 2018NRA, unlike its predecessor, also adopts a TF assessment of threat and vulnerabilities as well as a ML assessment. Where there is no Gibraltar specific issue or existing mitigation, Gibraltar has agreed with the EU assessment and scoring and adopted this as its own. However, in a number of areas existing mitigation is already in place and for these a different score has been adopted with an explanation provided as to why a lower score has been adopted. Conversely, there are also risks which for an international financial centre are higher and as such a higher score and explanation adopted.

2.1 EU Supra National Risk Assessment

The 2018NRA is based, to a very large extent, on the work of the EU's Supra National Risk Assessment (EUSNRA) and it therefore important that the EUSNRA be read and understood in framing the Gibraltar specific amendments and considerations. Gibraltar has a large number of mitigation measures in place for many of the threats identified in the EUSNRA as well as specific threats that are not covered by the EUSNRA. In framing the Gibraltar view of the EUSNRA these mitigation measures and specific threats have led to a revaluation of the risk scores for threats and vulnerability both in terms of Terrorist Financing and Money Laundering.

Readers of the 2018NRA should therefore be aware of the full text of the EUSNRA which can be downloaded from here;

http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=81272

2.2 Private and Public sector input

In arriving at a view for each of the risks, as well as the risks themselves, stakeholder public sector authorities as well as trade representative bodies in the finance sector and their member firms were invited to provide formal feedback on an early draft of the 2018NRA findings in April 2018.

The feedback received from the formal consultation process has been incorporated into the final version of the report.

2.3 Quantitative v Qualitative Data to support the findings

In reaching a final conclusion as to the risks and scoring there was a need to rely upon the experience and practices of law enforcement agencies, prosecutors and regulators who together with the regulated sectors in financial services, gaming and other professions, represent the coal-face in the prevention of ML and TF.

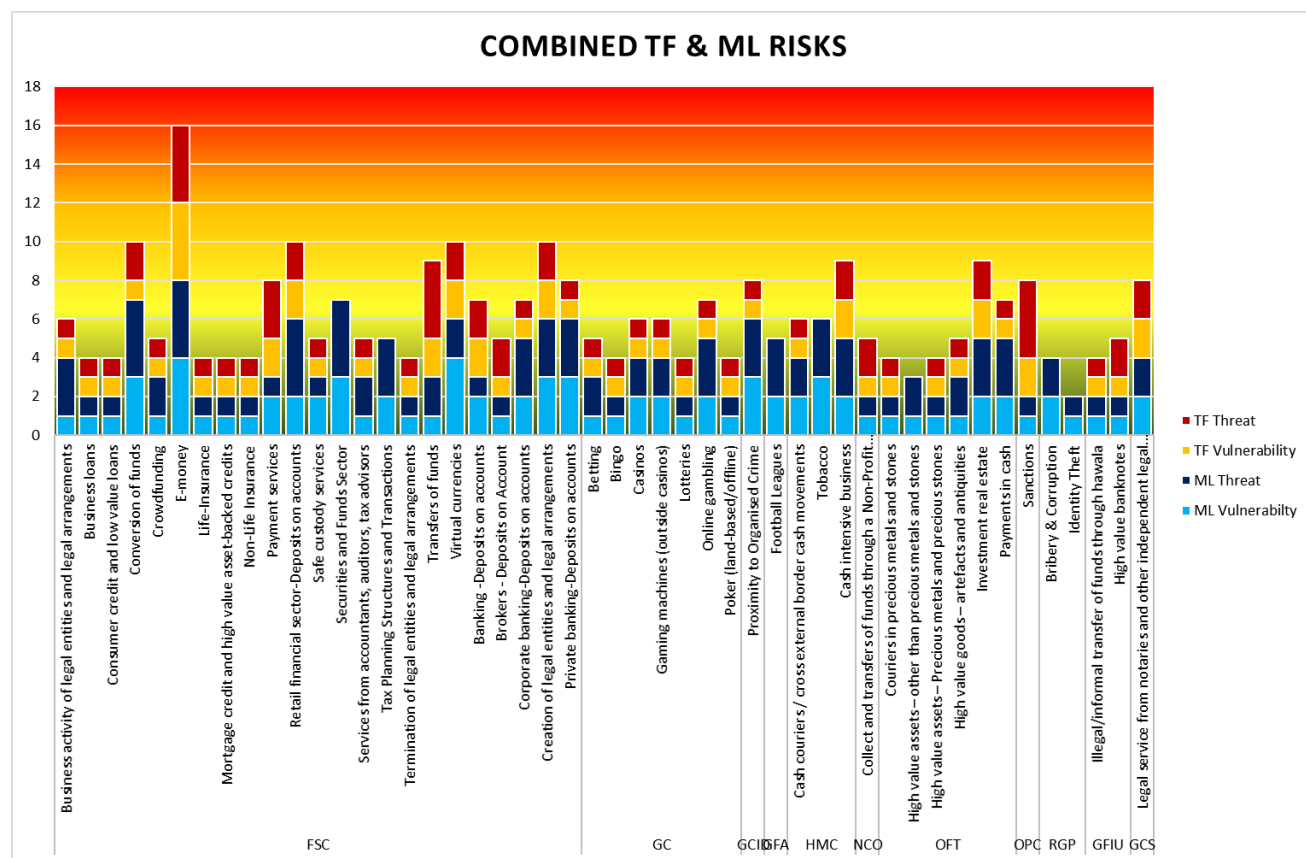
Supplementing the conclusions reached from qualitative data must be quantitative data that provides a fuller picture and reality check of fact v fiction. For the 2016 NRA authorities did not have a substantive data set to place reliance upon and the decision was taken in 2014 by HMGoG to adopt the OSCE Handbook on Data Collection in Support of Money Laundering and Terrorism Financing, National Risk Assessments² as the basis for data collection in Gibraltar. An analysis of the data collected via this methodology as well as the Financial Services Commission's (FSC) financial crime return is to be found below.

² <https://www.osce.org/eea/96398>

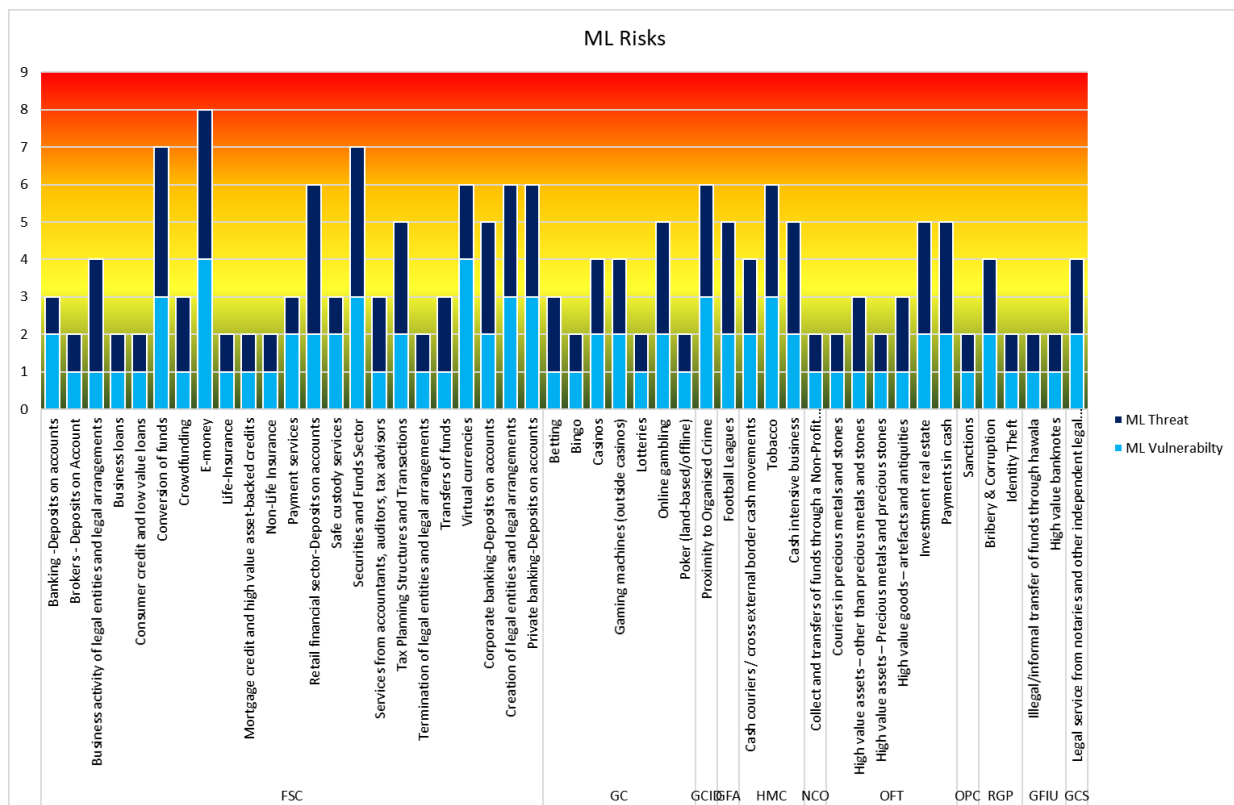


3 Key Risks

The 2018NRA combines both the ML score and the TF score for each risk to determine an overall risk score. The findings, grouped by the authority with primacy over ensuring the risks are mitigated are as follows;



There is some differentiation when ML and TF are looked at separately;





This puts Gibraltar's top 13 combined ML and TF risks as being;

- 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
- Sanctions

The annex to this report details each threat of the 2018NRA.

4 Supporting Data analysis

4.1 FIU STR Data

Information from the Suspicious Transaction Reports relating to ML suspicions submitted between 2014 to 2017 would indicate that the Gambling Industry is the activity which is most susceptible to ML. However, this is due to the large number of accounts operated by this sector and the high levels of submitted STRs are related to player related fraud.

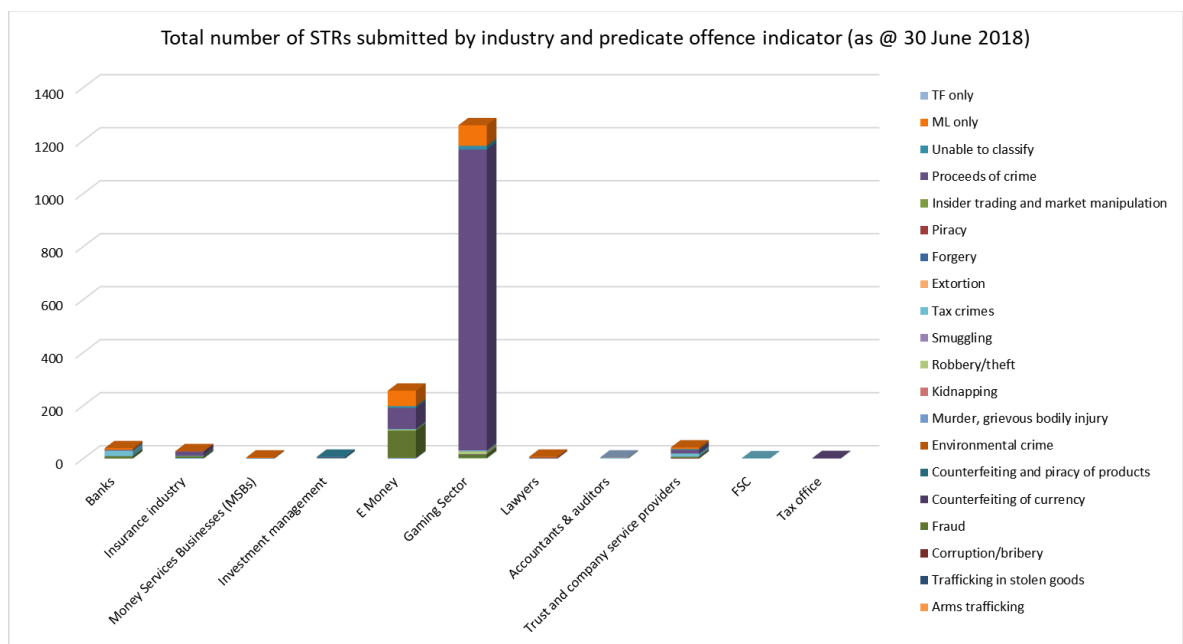
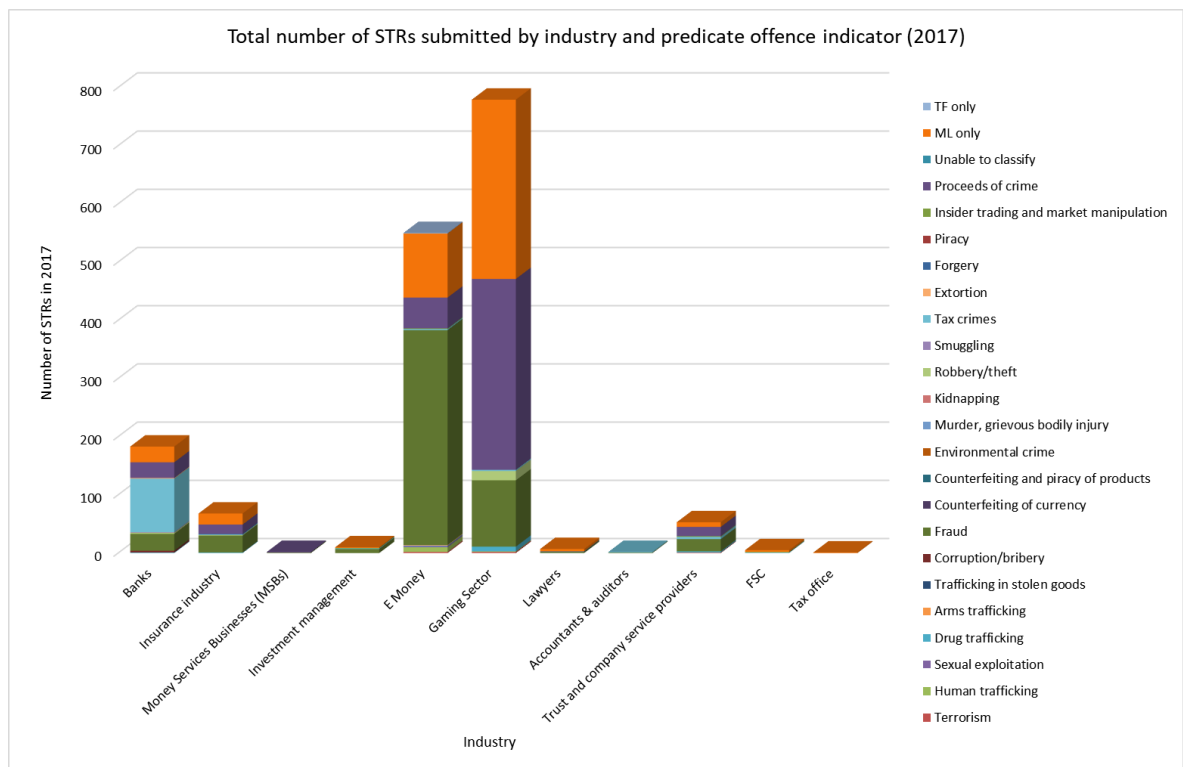
	2014	2015	2016	2017	Total
<i>Gambling Industry</i>	10	20	319	779	1128
<i>Banks</i>	32	21	43	183	279
<i>Non-bank deposit takers</i>	4	9	52	0	101
<i>E-Money</i>	0	0	0	550	550
<i>Trust and company service providers</i>	4	4	10	53	71
<i>Insurance industry</i>	4	1	6	68	79
<i>Lawyers</i>	1	2	3	7	13
<i>Money Services Businesses (MSBs)</i>	1	0	3	2	6
<i>Investment Management</i>	0	0	0	10	10
<i>Accounting & Auditors</i>	0	0	0	2	2
<i>Supervisory Authorities (GoG)</i>	0	0	0	6	6

On TF related STRs, the following data is available;

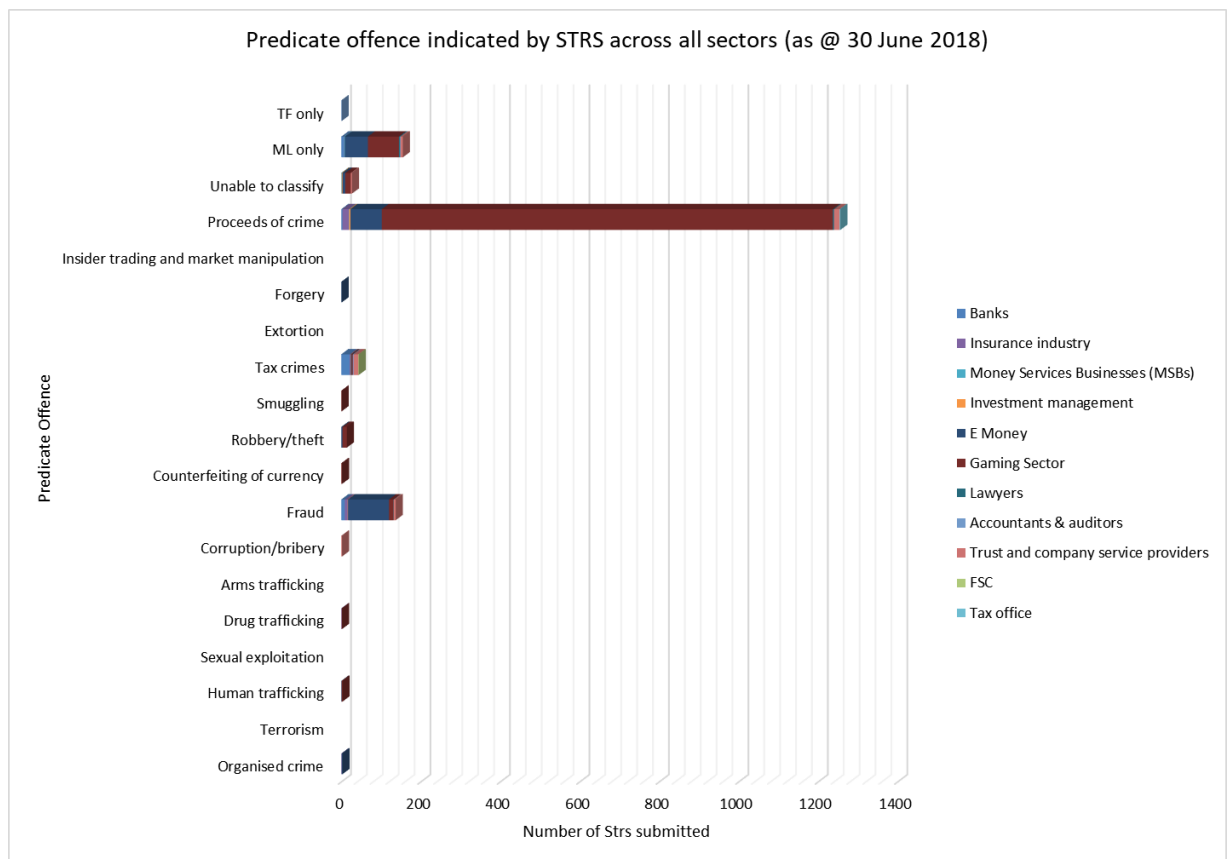
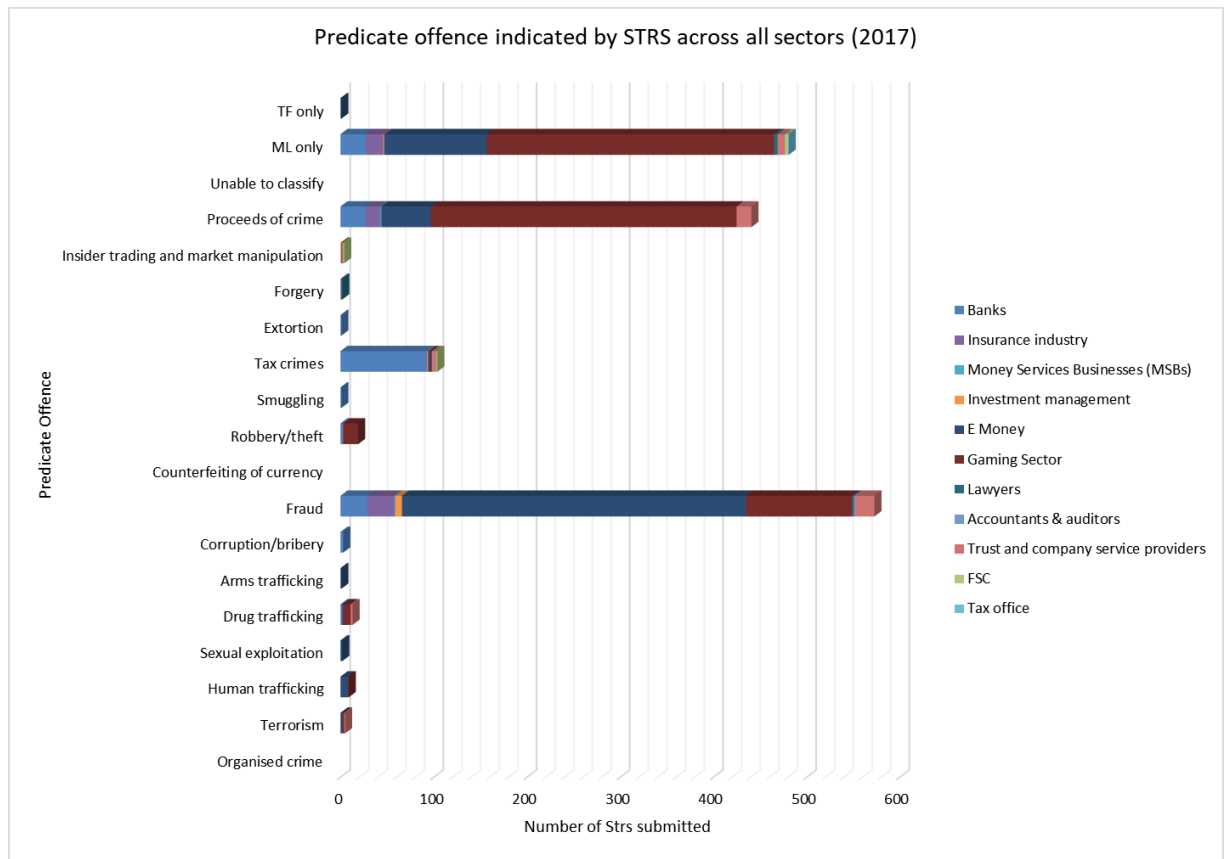
	2014	2015	2016	2017	Total
<i>Insurance industry</i>	6	12	1	0	19
<i>Gambling Industry</i>	0	2	5	0	7
<i>Money Services Businesses (MSBs)</i>	0	0	6	0	6
<i>Trust and company service providers</i>	0	1	2	0	3
<i>Banks</i>	1	1	0	0	2
<i>Non-bank deposit takers</i>	1	1	0	0	2
<i>E-Money</i>	0	0	0	1	1
<i>Accountants & auditors</i>	1	0	0	0	1

The relative high-level of insurance related TF STRs in 2015 relates exclusively to a number of false positives of names hitting the list of terrorist designated persons that arises due to the large client base of motor insurance business being written in the UK. All of these cases have been followed up and either proven to be false positives and where necessary information passed onto the relevant competent authorities overseas for further investigation although none have resulted in any action being taken. Subsequent refinement of the reporting processes of this sector has led to more accurate reporting.

An analysis of the STRs submitted, by indicated predicate offence and industry shows, as expected that the majority of the STRs are submitted by the Gaming, E-Money and Bank sectors which in line with the identified risks of the NRA and then the insurance and TCSP sectors which are also consistent with the risk profile and activities conducted in Gibraltar;



As far as the indicated predicate offences arising from the STRs are concerned, Fraud and Proceeds of Crime are the highest identifiable predicate offences (ML Only classification is given where no specific predicate offence can be assigned);

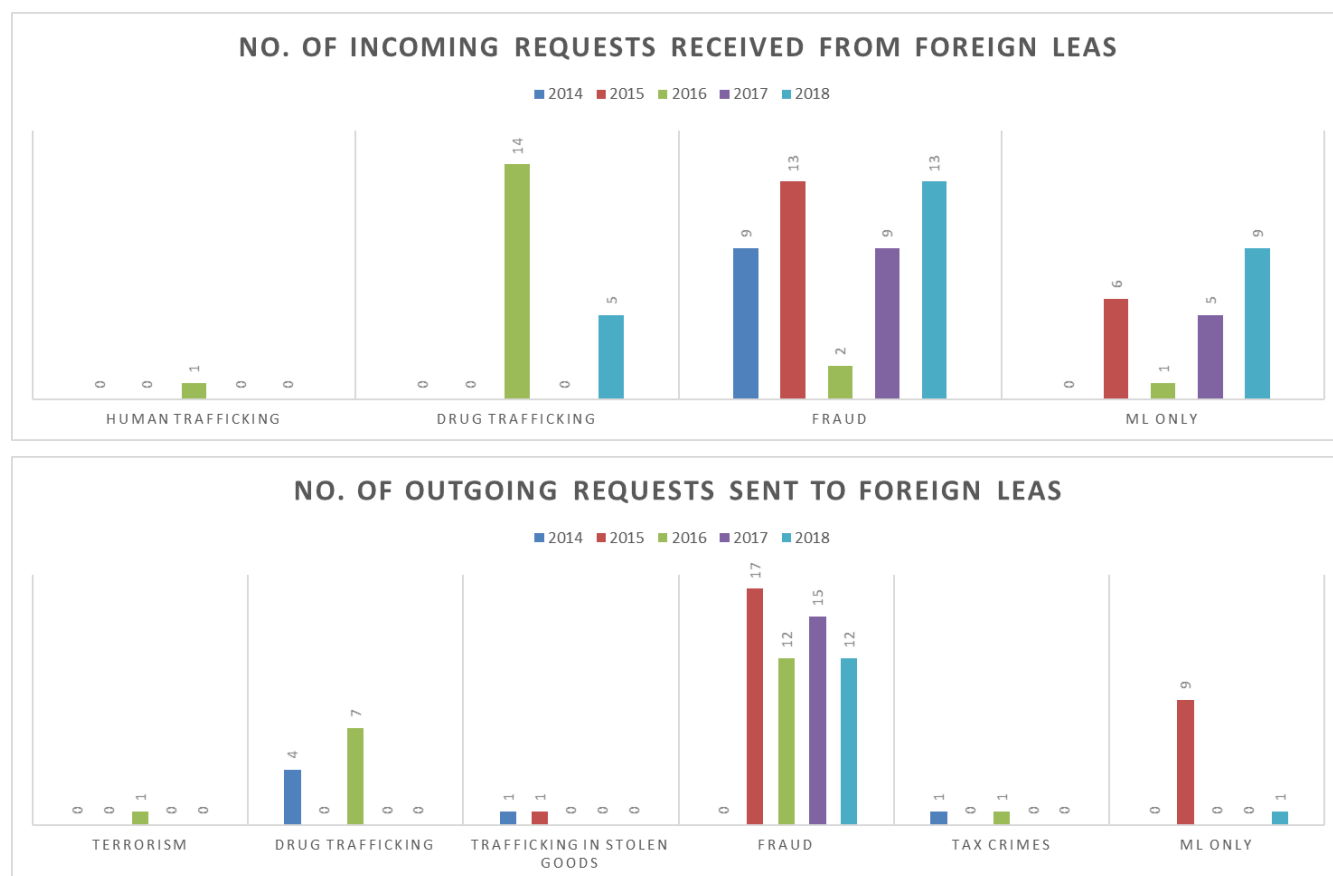


4.2 International Information Sharing Data

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.

4.2.1 Law Enforcement Exchanges

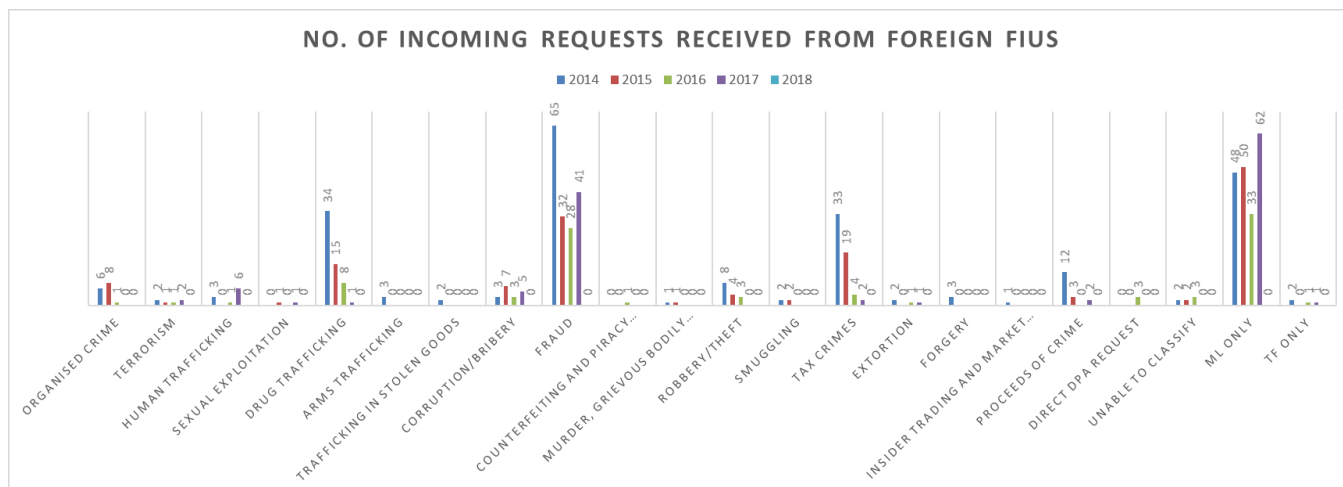
In looking at the exchange of information shared by Law Enforcement Agencies, the majority of requests have been related to Fraud, Drug Trafficking and Money Laundering with only one request in the four years examined relating to Human Trafficking and one outgoing request related to terrorism;





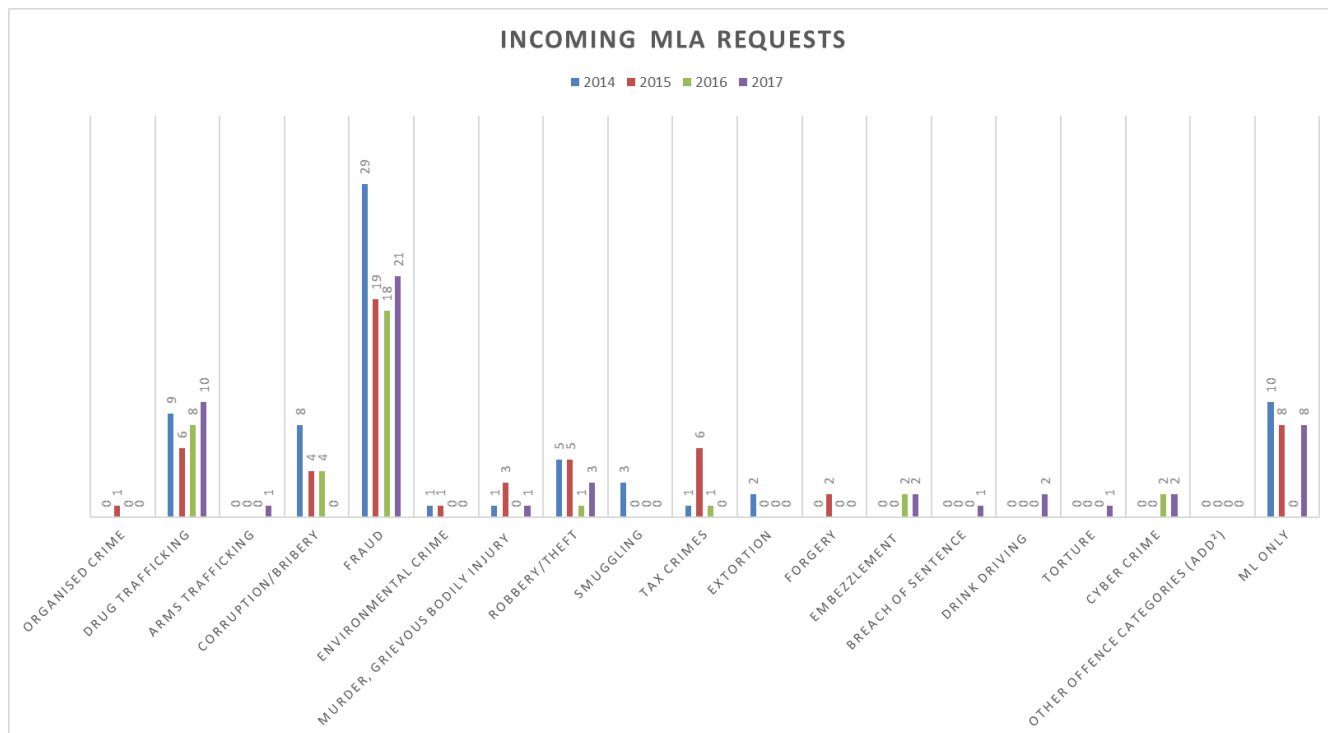
4.2.2 FIU Exchanges

A similar picture arises when looking at exchanges of information by the Gibraltar Financial Intelligence Unit with its counterparts;



4.2.3 MLA Requests

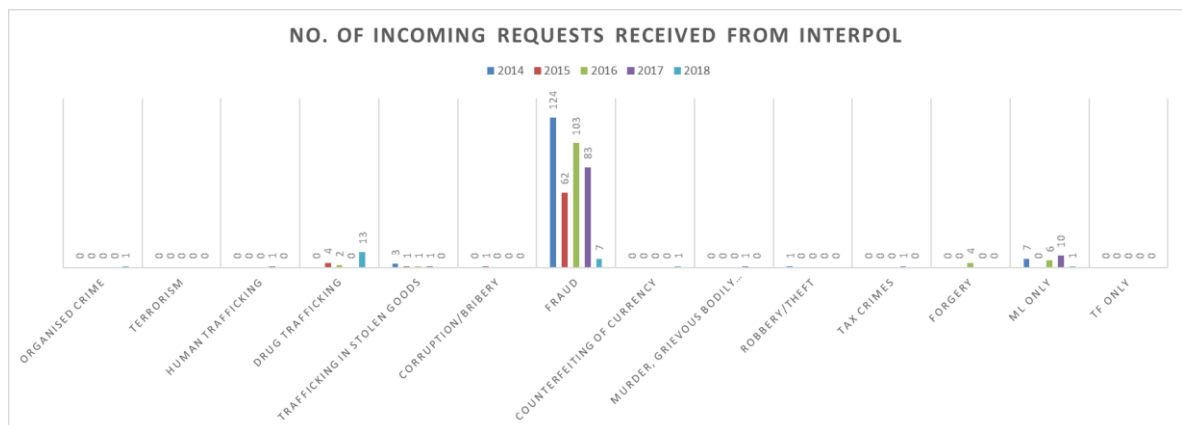
The formal Mutual Legal Request route for information exchange is also used extensively and the assistance sought shows;





4.2.4 Interpol Requests

Requests for intelligence via Interpol mechanisms also show similar patterns regarding the underlying predicate offences;



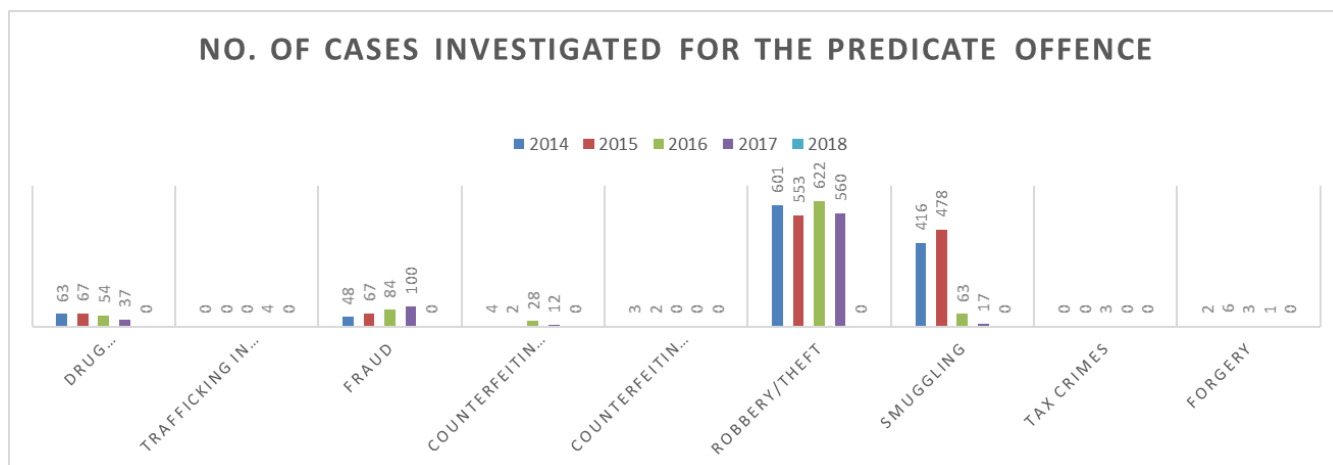
4.2.5 TF

It is important to note that there have only been 4 TF related exchange of information requests between 2014 and 2017 (2 in 2014 and one each in 2016 and 2017) and these have been handled via the FIU to FIU route.

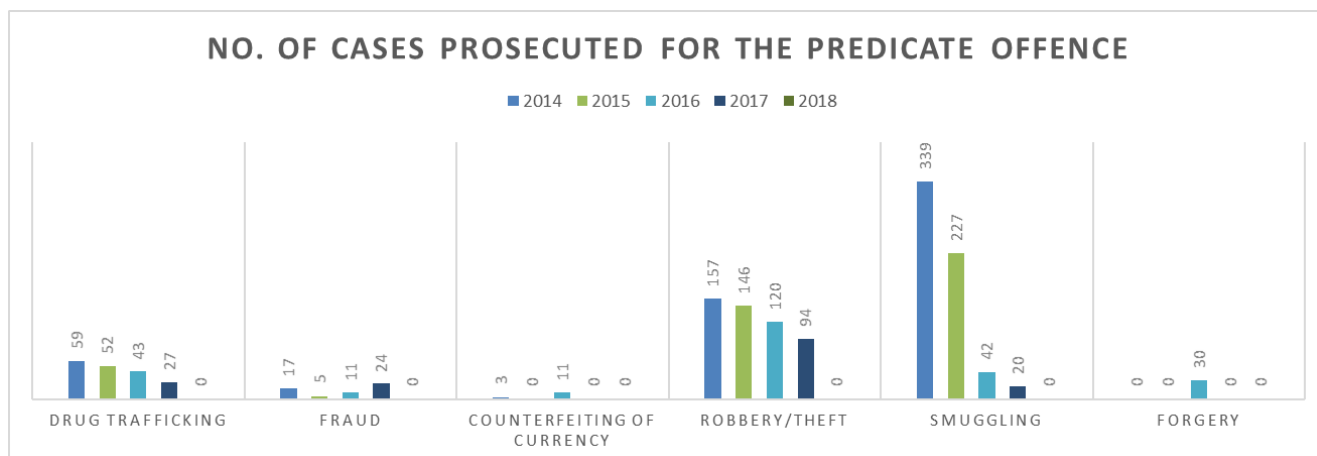


4.3 Investigation and Prosecution Data

The number of investigations brought to bear by LEAs for the predicate offence is also an important consideration to determine vulnerabilities that could lead to ML or TF.



Here the data corroborates the fact that most local criminal activity is that of theft and smuggling relating to the export of tobacco products. The number of prosecutions brought by the Crown is commensurate with the number of investigations commenced;





The ratio of convictions against prosecutions is also consistent;





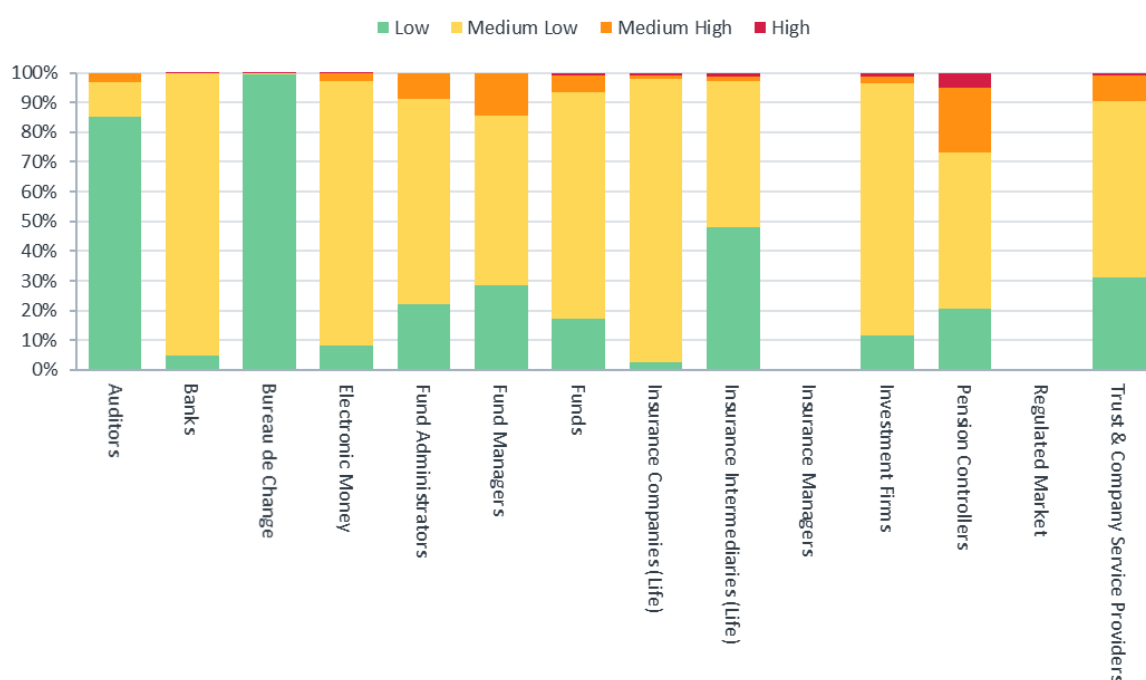
4.4 Financial Services Regulatory Data

As an international financial centre, Gibraltar's financial services industry deals with a non-resident client base. There is a need to ensure that in its financial dealings, firms who transact with potentially higher risk jurisdictions do so with increased awareness and higher mitigation to address these risks.

The FSC has collected data from regulated entities which shows that even though some transaction occurs with higher risk jurisdictions, these are few in comparison with the majority of the transactions that take place in Gibraltar.

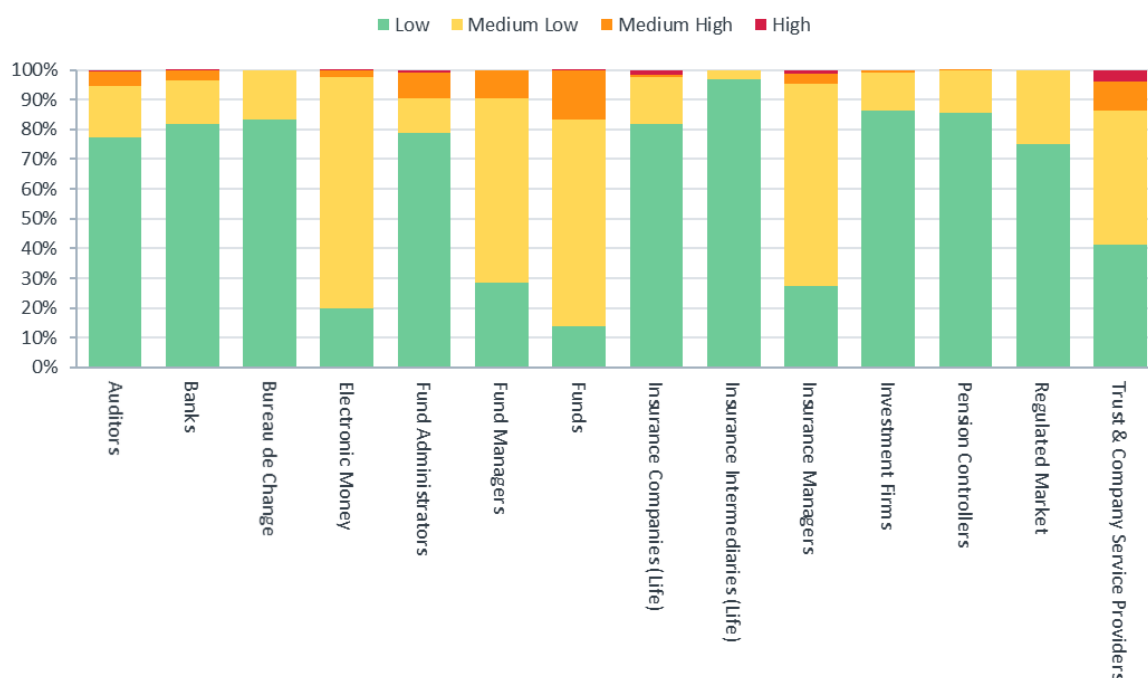
The following data extracts have been taken from the FSC's Financial Crime Return as at 30 June 2017.

Active individual customers by country of residence:

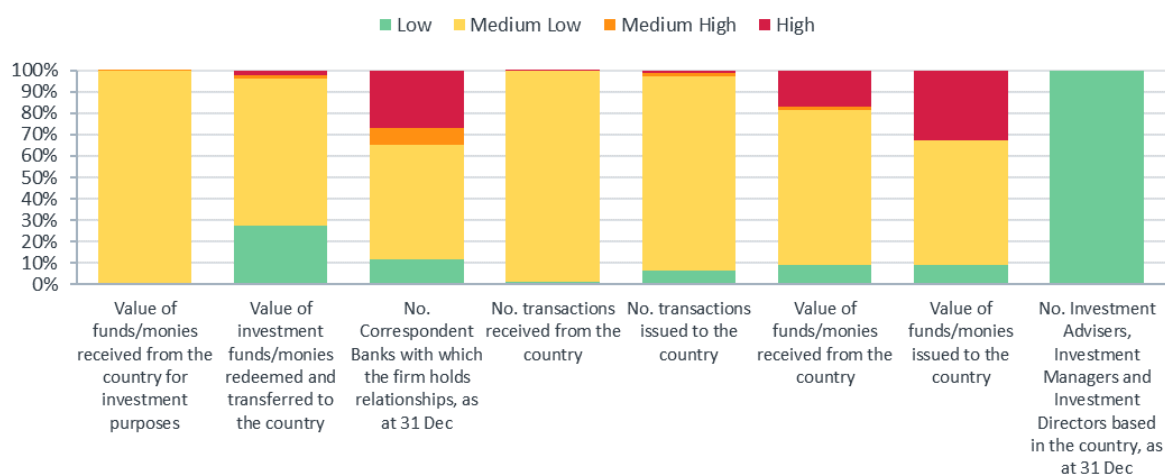




Active corporate customers by country of activity

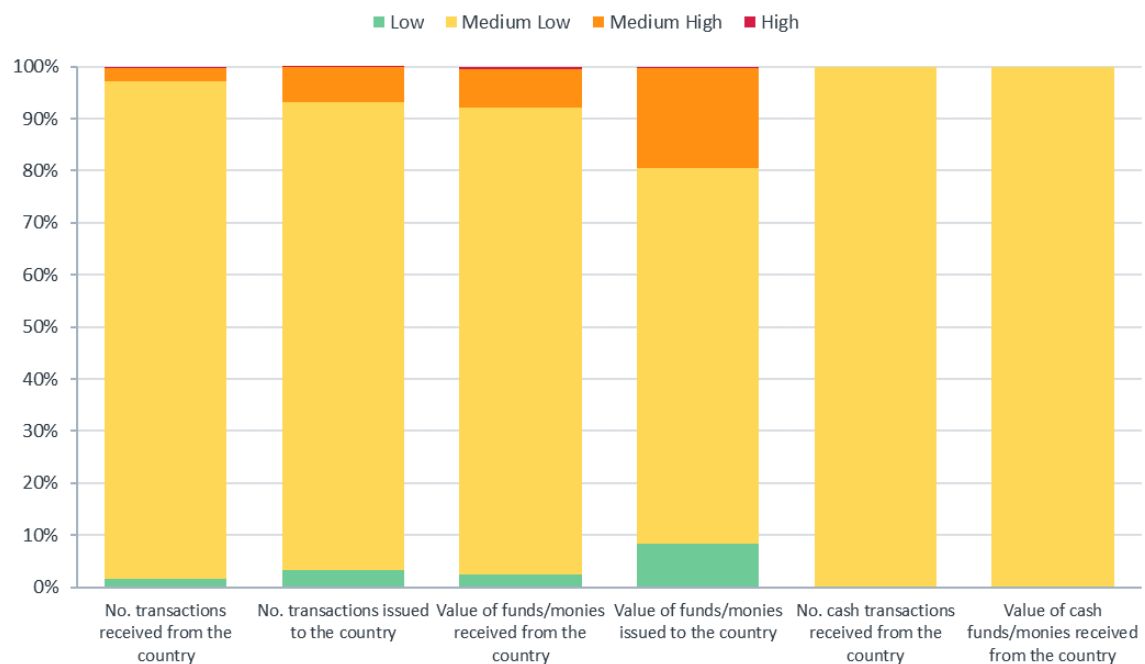


Specific data from the banking sector alone also shows the breakdown of their activities broken down by jurisdiction risk and activity being conducted;

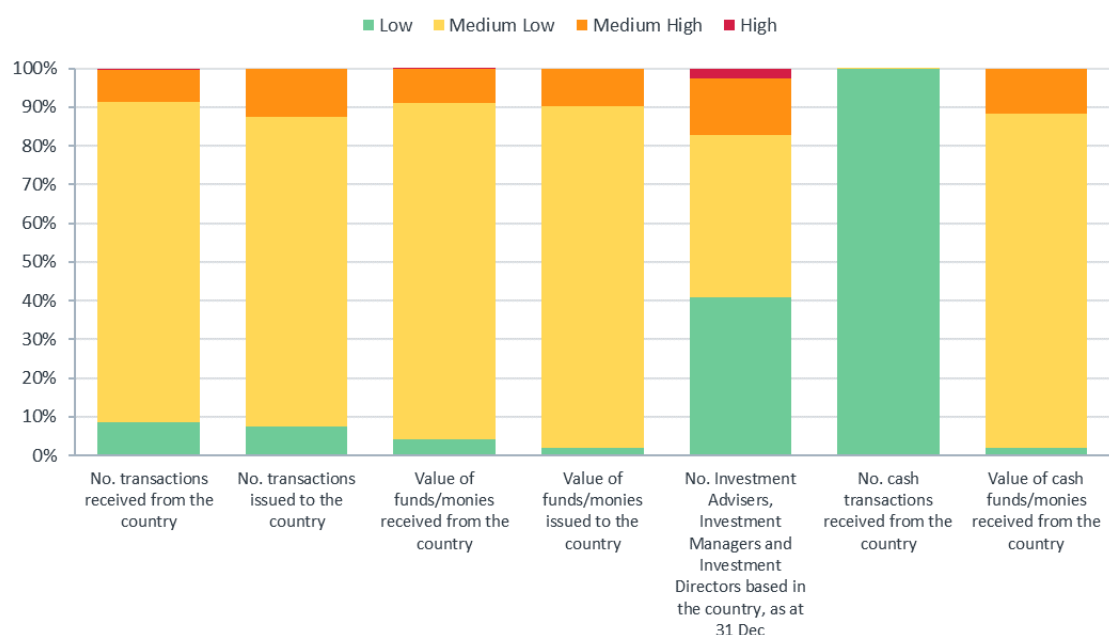




In the highest risk identified in the NRA, Electronic Money, the activity shows, that negligible amounts of funds transfer occurred with high risk jurisdictions;

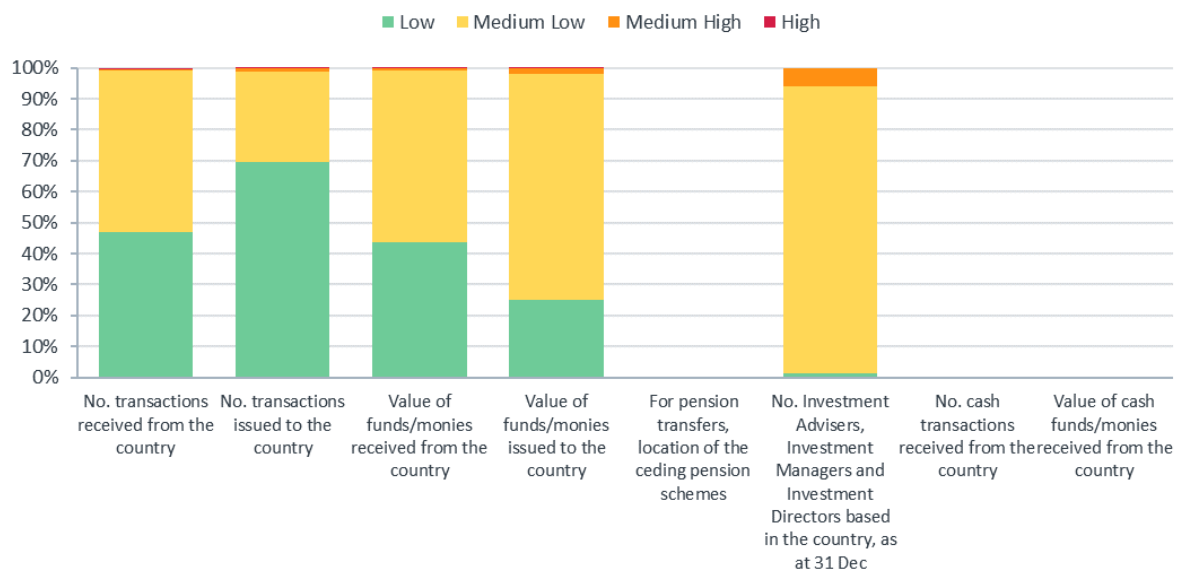


This pattern is also seen in the funds sector;





And in the life assurance sector;



Revision to the National Risk Assessment for Terrorist Financing and Money Laundering Risks

2018 National Risk Assessment

Legend:

TF or ML Risks

- 0 = Not Applicable
- 1 = Lowly Significant
- 2 = Moderately Significant
- 3 = Significant
- 4 = Very Significant

Legend:

Total ML or TF Risk

 <=7 - Low Risk

 8-10- Medium to Low Risk

 12-13 - Medium High Risk

 =>14 - HighRisk

Total Risk Score	16
Risk ID	18
Risk Name	E-money
Description	Perpetrators use characteristics and features of some of new payment methods "directly" using truly anonymous products (i.e. without any customer identification) or "indirectly" by abusing non-anonymous products (i.e. circumvention of verification measures by using fake or stolen identities, or using straw men or nominees etc.) Perpetrators can load multiple cards under the anonymous prepaid card model. This multiple reloading could lead to substantial values which can then be carried out abroad with limited traceability. Gibraltar Assessment Pre-paid debit and or credit cards are a form of e-money. There are five e-money/card issuers operating from Gibraltar at present and these are seen as presenting growth opportunities for the finance sector. Part of the attractiveness of e-money products is to facilitate access to the financial market to those excluded from mainstream banking services, those of low income, children and those who want to make use of on-line services who might otherwise not have an established bank account etc. It also has the advantage of reducing cash handling costs and the holding of cash in a society. Cards may typically be acquired at retail outlets and could be bought for a cash equivalent in exchange for a "load" or e-money value of the same amount. However, anonymous 'cash loading' is extremely restricted by EU law that also applies in Gibraltar. Some of these lower value cards can be bought anonymously or without the production of any due diligence and id verification requirements that would normally be found in the opening of a bank account, for example.
Terrorist Financing Risk Assessment	
Threat	The assessment of the TF threat related to e-money shows that the use of e-money can be particularly attractive for terrorist groups, as it allows funds to be moved easily and anonymously (in particular with prepaid cards instead of bulk of cash). In practice, e-money is rather easy to access and does not require specific expertise or planning. This is even more the case for non-account based e-money products. As far as the use for TF purposes is concerned, LEAs have gathered evidence that e-money loaded onto prepaid cards has been used to finance terrorist activities, in particular to assist the terrorists in committing their actions (hotel or car rentals). However, the level of TF threat presented by e-money shall be assessed proportionally to the level of threat represented by cash which constitutes a more competitive and more attractive tool because it is easier to access than e-money. In that sense, cash is still the preferred option to finance travels to war zones. At the same time, e-money loaded onto prepaid cards may be seen by terrorist groups as more secure as it allows more discrete payments than cash. They may also see this option as more attractive when cash transactions are not an available option (e.g. online transactions, online purchases).
Threat Score	4
Vulnerability	This sector is particularly appealing given the high level of cash transactions and the use of pre-paid and/or anonymous cards. The risk exposure within this area is heightened given the significant volumes of products and services which facilitate speedy or anonymous transactions and the significant volume of higher risk customers. The industry, however, has a sound awareness of the risks posed and in general, implements adequate measures and procedures to manage/mitigate the risks posed.
Vuln. Score	4
	8

Money Laundering Risk Assessment

Threat

There are five e-money/card issuers operating from Gibraltar at present and these are seen as presenting growth opportunities for the finance sector. Part of the attractiveness of e-money products is to facilitate access to the financial market to those excluded from mainstream banking services, those of low income, children and those who want to make use of on-line services who might otherwise not have an established bank account. It also has the advantage of reducing cash handling costs and the holding of cash in a society. Cards may typically be acquired at retail outlets and could be bought for a cash equivalent in exchange for a "load" or e-money value of the same amount. Some of these lower value cards can be bought anonymously or without the production of any due diligence and identity verification requirements that would normally be found in the opening of a bank account, for example. However, anonymous 'cash loading' is extremely restricted by EU law that also applies in Gibraltar.

Additionally, this is an area which is often exploited for unauthorised activity purposes which increases the ML risk further.

Threat Score

4

Vulnerability

In criminal activity it is not uncommon for payments to be effected across borders. Payment for these transactions used to entail the physical transportation of cash from one to the other but can also be carried out using these cards, in lieu of cash. Once the card has been loaded the holder is able to integrate these funds into the financial system through the use of the credit cards to purchase goods and services in a manner which does not identify him as the purchaser. However, the severe restrictions on anonymous cash loading do make significant amounts of activity highly cumbersome. Where prepaid cards do require CDD the sophistication of service providers technology allows for rapid responses to requests for evidence from other jurisdictions. This ability to rapidly assist LEA's make the use of this type of product less attractive than cash.

The E-money industry is attractive given the use of anonymous cards and potential opacity in tracing the origin of the funds loaded. However, in Gibraltar, there are restrictions on anonymous 'cash loading' which make significant amounts of activity highly cumbersome.

The industry, however, has a sound awareness of the risks posed and in general, implements adequate measures and procedures to manage/mitigate the risks posed.

Vuln. Score

4

8

Total Risk Score	10
Risk ID	17
Risk Name	Conversion of funds
Description	Perpetrators are converting their funds into another currency to facilitate the conversion, transfer or laundering of funds.
Terrorist Financing Risk Assessment	
Threat	The EU TF threat assessment highlights that terrorists exploit this modus operandi particularly using the conversion of EUR/USD which rarely takes place in Gibraltar. From a technical aspect, this sector does not require a high level of expertise, knowledge or specific planning which increases the risk. However, there is little to no evidence to suggest that this industry is being exploited for TF purposes.
Threat Score	2
Vulnerability	This sector does not require much expertise or knowledge which makes it attractive to perpetrators. Given the high level of cash transactions and the element of anonymity, this increases the vulnerability of this risk.
	The majority of the transactions are completed by locals or Spanish workers and are primarily one off transactions due to the cross-border nature of the jurisdiction and there are no locals or Spanish employees on the UN Sanctions lists. The remaining minority are tourists which arrive through passport controlled borders or via cruise ships where there is a pre-vetting process of all passengers. Therefore, the likelihood of this risk materialising is minimal
Vuln. Score	1
	3

Money Laundering Risk Assessment

Threat	Internationally, money remittance and currency exchange businesses have been both willing and unwilling participants in laundering activities, in all three stages of the process (placement, layering and integration). Gibraltar exchange business is mainly concerned with payment of wages and retail sector catering for the tourism industry. Gibraltar's cash based tobacco retail trade generates large volumes of Euros both with retailers and wholesalers. The threat of ML is two fold. Firstly in the exchange of Euros for sterling by the retailers direct to the public, and secondly in the wholesale of exchange of Euros by the retailers and wholesalers to legitimately GFSC licensed currency exchangers. Criminals recurrently exploit this modus operandi for ML purposes especially given that the sector is perceived as appealing and easy to abuse. Gibraltar's exchange business mainly concerns the payment of wages and retail sector catering for the tourism industry. Additionally, this is an area which is often exploited for unauthorised activity purposes, where individuals or entities are offering and/or providing the licensed services without being authorised to do so.
Threat Score	4
Vulnerability	ML through currency exchanges poses a number of regulatory and enforcement challenges. There is a level of risk awareness amongst the sector and the FSC works closely with it to ensure that the requirements are complied with including the management/mitigation of the potential risks. Clearly, laundering through money remittance and currency exchange providers poses a number of regulatory and enforcement challenges. At the same time, there is low detection of money laundering in comparison to the size of the

industry as a whole. In mitigation, money transmitters and currency exchanges are regulated and subject to on-site inspections. The vulnerability is increased due to the non-regulated sector conducting currency exchange on a wide scale without licences.

Licensees are required to submit quarterly returns which indicate the number and value of transactions, including those below €5,000, the sourcing of currency and destination of transactions.

Vuln. Score

3



Risk ID	22
Risk Name	Virtual currencies
Description	ML: Perpetrators use virtual currency systems traded on the internet to transfer funds or purchase goods anonymously (cash funding or third-party funding through virtual exchangers). TF: Virtual currency systems can be traded on the internet, are generally characterised by non-face-to-face customer relationships, and may permit anonymous funding or purchase (cash funding or third-party funding through virtual exchangers that do not properly identify the funding source). They may also permit anonymous transfers, if sender and recipient are not adequately identified.

Terrorist Financing Risk Assessment

Threat	LEAs have gathered some information according to which terrorist groups may use virtual currencies to finance terrorist activities. However, the use of virtual currencies requires technical expertise which makes it less attractive.
Threat Score	2
Vulnerability	Gibraltar has implemented a regulatory framework for digital ledger technology which requires authorisation to conduct in or from within Gibraltar (with effect from 1/1/2018). The supervisory framework is based on 9 Regulatory Principles. Principle 8 (AML/CFT measures) requires providers to have systems in place to prevent, detect and disclose financial crime risks such as money laundering and terrorist financing. DLT Providers must adequately apply anti-money laundering and counter terrorist financing preventive measures which are commensurate with their risks, including having appropriate systems for the reporting of suspicious activity. DLT Providers need to comply with the Proceeds of Crime Act 2005 (POCA), which transposes the 4th money laundering EU Directive and international standards as set out by FATF.
Vuln. Score	2
	4

Money Laundering Risk Assessment

Threat	Few investigations have been conducted on virtual currencies which seem to be rarely used by criminal organisations. While they may have a high intent to use due to VCs characteristics (anonymity in particular), the level of capability is lower due to high technology required. Prepaid credit card operators offer services where VC's are connected to credit cards. This allows for the access to fiat currency through credit cards.
Threat Score	2
Vulnerability	Gibraltar has implemented a regulatory framework for digital ledger technology which requires authorisation to conduct in or from within Gibraltar (with effect from 1/1/2018). The supervisory framework is based on 9 Regulatory Principles. Principle 8 (AML/CFT measures) requires providers to have systems in place to prevent, detect and disclose financial crime risks such as money laundering and terrorist financing. DLT Providers must adequately apply anti-money laundering and counter terrorist financing preventive measures which are commensurate with their risks, including having appropriate systems for the reporting of suspicious activity. The vulnerability caused by VC being accessible through credit cards is reduced due to this service requiring CDD to operate. The prepaid card providers have well established systems for data retrieval and are fully compliant with LEA data requests making them less vulnerable to this risk. DLT Providers need to comply with the Proceeds of Crime Act 2005 (POCA), which transposes the 4th money laundering EU Directive and international standards as set out by FATF.
Vuln. Score	4
	6

Risk ID	11
Risk Name	Retail financial sector-Deposits on accounts
Description	Perpetrators place the proceeds of crime into the financial system through the regulated credit and financial sector in order to hide its illegitimate origin. Terrorists, supporters or facilitators place funds from legitimate sources into the financial system with a view of using it for terrorist purposes. Money mules mechanisms may be used to transfer proceeds out of the banking sector using personal accounts either through cybercrime (scamming, fake banking websites etc.), money value transfer services.

Terrorist Financing Risk Assessment

Threat	A high level of awareness, mature KYC process and regulatory framework in Gibraltar's FI sector mitigates the risk considerably. There have also been no known uses of Gibraltar deposit accounts by Terrorist Groups or being used for TF activities. Furthermore, there is no evidence of the use of money mule mechanisms in Gibraltar.
Threat Score	2
Vulnerability	Although the risk exposure may be considered as quite high (significant level of transactions), the sector shows a good level of awareness to the risk vulnerability and is able to put in place the relevant red flags. The legal framework and controls are the basis of a good level of reporting.
Vuln. Score	2
	4

Money Laundering Risk Assessment

Threat	The assessment of the ML threat related to deposits on account /retail banking shows that this risk scenario concerns both placing funds and withdrawing funds (i.e. deposits on account and use of this account). It is frequently used by organised crime organisations but also by relatives/close associates which extends the scope of the intent and capability analysis. Law enforcement authorities reported a frequent use of this modus operandi since it one of the easiest way to integrate illicit funds into the financial system. It does not require planning and knowledge of how banking systems work, and it is low cost. Also complex money laundering cases were reported with funds deposited on accounts transiting via a chain of complex operations. For such complex schemes, perpetrators may use available expertise from intermediaries.
Threat Score	4
Vulnerability	Similarly to what has been analysed under the TF vulnerability part, deposits on accounts are less exposed to ML risks due to the good functioning of the controls and a good level of awareness from the sector. Furthermore, there is no evidence of the use of money mule mechanisms in Gibraltar.
Vuln. Score	2
	6

Risk ID	29
Risk Name	Creation of legal entities and legal arrangements
Description	Perpetrators create complex structures involving many jurisdictions, in particular offshore jurisdictions with secretive chains of ownership where the owner of another company or another legal structure is registered elsewhere. Nominees are designated and will only appear to be in charge of the company by hiding the link with the true beneficial owner. By involving offshore companies, the perpetrators can stay anonymous, return the funds derived from criminal activity into the legal economy, and commit tax fraud, tax evasion and other activities that impair the state budget or conceal the sources of the funds. This involves the creation of 'opaque structures', defined as structures where the true identity of the owners(s) of entities and arrangements in that structure is concealed through the use of nominee directors for instance. In such cases, it is the nominee director who only appears to be the beneficial owners of the company .
Terrorist Financing Risk Assessment	
Threat	While few cases of exploitation of this modus operandi for TF purposes have been identified, the technical expertise and knowledge required is high, and may thus dissuade terrorist organisations which may prefer simpler and more accessible solutions. There is little evidence to suggest that Gibraltar has experienced any TF cases within the TCSP sector to date. However, this is a common modus operandi for criminals to exploit.
Threat Score	2
Vulnerability	The TCSP industry in Gibraltar has a level of awareness of the TF risks posed and these are factored in to its methodologies and assessments. The TCSP industry in Gibraltar is a long standing sector which has been regulated for many years.
Vuln. Score	2
	4

Money Laundering Risk Assessment

Threat	The guise of commercial structuring or tax planning may be used as a cover for otherwise illicit uses. Without understanding the real rationale for tax planning structures a TCSP may be unable to make an accurate determination of the rationale for the use of the Gibraltar legal entity and be misinformed as to the true purpose of the structure. Corporate vehicles and trusts could be abused to provide an additional layer of opacity between perpetrators of a criminal activity and the act itself. Firms should always be wary of customers wishing to seek to establish such structures which have no apparent economic reason or link to the jurisdiction. Legal structures are frequently used internationally in the layering and integration stages of money laundering. There is little, if any, evidence of this occurring in Gibraltar in relation to TF. Unlicensed TSCP activity poses a substantial threat due to the absence of supervision from the GFSC. Incidents will only come to the attention of authorities for executive action following the receipt of intelligence whether this be through a SAR or other means.
Threat Score	3
Vulnerability	Gibraltar has a respected, regulated, well-established and important Trust and Corporate Service Providers (TCSP) sector. Gibraltar legal entities are commonly used both as asset holding, investment and transactions based vehicles for both the domestic as well as, international community. The same applies to corporate entities formed elsewhere but managed and/or controlled from within Gibraltar.

All TCSPs are required to be licensed and are regulated by the Financial Services Commission. Gibraltar is fully up to date in meeting its international obligations in transparency and exchange of information and is fully compliant with European Union legislation. The ability for private individuals to register companies with Companies House affords the opportunity for unlicensed TSCP's to conduct a business.

The jurisdiction has recently implemented the UBO register. This decreases the identification vulnerabilities and risk of the creation of an opaque structure.

Vuln. Score

3

6

Total Risk Score	9
Risk ID	36
Risk Name	Investment real estate
Description	Perpetrators are laundering the proceeds of crime in the country by investing in the real estate sector. Perpetrators purchase an asset at below market price, paying the difference to the seller under-the-table in cash. Under or over valuation of property: back-to-back loan which may involve financial institutions or mortgage schemes. Perpetrators may invest, as non-resident, in a country (through visa systems) and develop ML/TF network (including via the complicit legal professionals)
Terrorist Financing Risk Assessment	
Threat	REAs within Gibraltar only receive a commission on the purchase which is usually between 1 and 2% of the purchase price. Purchase cash moves instead through lawyers' client account, decreasing the attractiveness to criminals of REAs for laundering and therefore reducing the threat.
Threat Score	2
Vulnerability	OFT outreach programmes, their meeting with every REA to discuss AML/CFT issues and the issuance of detailed guidance notes considerably reduces the vulnerability of the jurisdiction. All licensed REAs are required to report annually to the OFT, implement internal systems of control and other requirements in order to mitigate their risk.
Vuln. Score	2
	4
Money Laundering Risk Assessment	
Threat	REAs within Gibraltar only receive a commission on the purchase which is usually between 1 and 2% of the purchase price. Purchase cash moves instead through lawyers' client account, decreasing the attractiveness to criminals of REAs for laundering and therefore reducing the threat.
Threat Score	3
Vulnerability	OFT outreach programmes. The OFT is meeting with every REA to discuss AML/CFT issues and the issuance of detailed guidance notes considerably reduces the vulnerability of the jurisdiction. All licensed REAs are required to report annually to the OFT, implement internal systems of control and other requirements in order to mitigate their risk. In addition, the distinct lack of substantial numbers of high value properties to make large scale acquisitions are not viable due to the fact that our market is very small compared to other jurisdictions, despite the relatively high value of properties.
Vuln. Score	2
	5

Risk ID	8
Risk Name	Cash intensive business
Description	Cash intensive business is used by perpetrators: -to launder large amounts of cash, which are proceeds of criminal activity, by claiming that the funds originate from economic activities; -to launder amounts of cash, which are proceeds of criminal activity, by justifying its origin based on fictitious economic activities (both for goods and services) -to finance, through often small amounts of cash, terrorist activities without any traceability This risk scenario is intrinsically linked to use of/payment in cash and to high value denomination banknotes risk scenario.

Terrorist Financing Risk Assessment

Threat	The elements gathered by the LEAs and FIUs show only few cases have been registered meaning that terrorist groups do not favour this risk scenario as it requires some technical expertise and investments to run the business in itself which makes this modus operandi less attractive.
Threat Score	2
Vulnerability	Gibraltar's retail sector is low level/volume and not cash intensive therefore Gibraltar's Vulnerability assessment is lower than the EU's.
Vuln. Score	2
	4

Money Laundering Risk Assessment

Threat	There exists the possibility of a number of business being established and operated for the purposes of integrating cash generated from proceeds of crime.
Threat Score	3
Vulnerability	Due to low level of cash generating predicate offences being committed in Gibraltar there is little likelihood that any such businesses would be yielding large amounts of cash inputs.
Vuln. Score	2
	5

Risk ID	19
Risk Name	Transfers of funds
Description	ML: Perpetrators may use MVTs services: -to comingle funds from legitimate/illegitimate customers (fake ID, fake invoices, ...) - to launder proceeds of crime through settlement systems in a third country (using passporting). MVTs channel funds through highly complex payment chains with a high number of intermediaries and jurisdictions involved in the funds circuit, thereby hindering traceability of illicit funds. MVTs operating throughout the payment chain often establish formal and/or informal settlement systems (frequently along with trade-based money laundering techniques) also hampering traceability of illicit funds. -to break large sums of cash into smaller amounts that can be sent below the thresholds where stricter identification of the customer is required -to place the proceeds of crime into the financial system through the regulated MVTs offering payment accounts or similar products. Perpetrators may also use such regulated MVTs providers to channel their funds -to place and/or transfer their funds, through money remittance services. Risks of ML/TF activity may be particularly high when funds to be transferred are received in cash or in anonymous e-money TF: Perpetrators use money and value transfers services provided by financial institutions to place and/or transfer funds that are in cash or in anonymous e-money (non-account based transactions). They use MVTs services to transfer rapidly amounts across jurisdictions, usually favouring a series of low amounts transactions to avoid raising red flags.

Terrorist Financing Risk Assessment

Threat	The assessment of the TF threat related to money value transfers services shows that terrorist groups recurrently use this modus operandi. LEAs and FIUs have gathered strong evidence that these services are used to collect and transfers funds which support the financing of terrorist activities, both within the EU and in particular to transfer funds by/for foreign terrorist fighters travelling to/from the conflict zones. MVTs are, depending on their organisation, easy to access and terrorists do not require specific expertise or techniques to abuse this service for finance terrorist activities. Terrorists might be more attracted to use large MVTs due to its global network of agents, whilst smaller MVTs might not be so attractive since they usually operate in a limited number of countries. Due to their features (see vulnerabilities part), MVTs are perceived as attractive and secure.
Threat Score	4
Vulnerability	Gibraltar generally agrees with the EU TF Vulnerability assessment but has not seen any evidence of these business being used for TF activities.
Vuln. Score	2
	6

Money Laundering Risk Assessment

Threat	There is no evidence to suggest that local MVTs are being used by Organised crime groups. MVTs are relevant financial businesses under POCA.
Threat Score	2
Vulnerability	There is no evidence to suggest that the MVTs operating in Gibraltar are being used or targeted for ML funds transfers.
Vuln. Score	1
	3

Total Risk Score	8
Risk ID	38
Risk Name	Legal service from notaries and other independent legal professionals
Description	Perpetrators may employ or require the services of a legal professional (such as lawyers, notaries and other independent legal professions) with a more or less level of involvement of the legal professional himself: - misuse of client accounts, -purchase of real property, -creation of trusts and companies/ management of trusts and companies, -undertaking certain litigation They may be involved in ML schemes through the creation of 'opaque structures' defined as business structures where the real identity of the owner(s) of entities and arrangements in that structure is concealed through the use of, for example, nominee directors. The creation of such structures often set up in multiple jurisdictions including offshore centres is complicated and requires both regulatory and tax services of professionals.
Terrorist Financing Risk Assessment	
Threat	The assessment of the TF threat related to legal service from legal professionals has been considered in conjunction with ML schemes related to legal service from legal professionals in order to hide the illegal origin of the funds. In that context, the TF threat does not benefit from a separate assessment.
Threat Score	2
Vulnerability	The assessment of the TF vulnerability related to legal service from legal professionals has been considered in conjunction with ML schemes related to legal service from legal professionals in order to hide the illegal origin of the funds. In that context, the TF threat does not benefit from a separate assessment.
Vuln. Score	2
	4

Money Laundering Risk Assessment

Threat	Criminals seek out the involvement of legal professionals in their ML/TF activities in what appear or are represented to be normal commercial transactions, to access specialised legal and notarial skills and services which could assist in the laundering of the proceeds of crime and the funding of terrorism.
Threat Score	2
Vulnerability	There are a number of ML/TF methods that commonly employ or, in some countries, require the services of a legal professional. Inherently these activities pose ML/TF risk. When clients seek to misuse the legal professional's services in these areas, they may be vulnerable. The methods include: •misuse of client accounts •purchase of real property •creation of trusts and companies •management of trusts and companies If the legal professional lacks understanding of the ML/TF vulnerabilities and red flag indicators, they are less able to prevent the misuse of their services. The legal profession is regulated for AML/CFT by the Registrar of the Supreme Court/ LSRA.
Vuln. Score	2
	4

Risk ID	21
Risk Name	Payment services
Description	Perpetrators are using the banking and financial system to channel their funds through bank accounts, wire credit and debit transfers, (peer-to-peer) mobile payments and Internet-Based Payment Services. Gibraltar Assessment Internationally, money remittance and currency exchange businesses have been both willing and unwilling participants in laundering activities, in all three stages of the process (placement, layering and integration), and in certain instances, for terrorist financing purposes. There are also links between money laundering in the money remittance sector and other criminal activities (e.g., fraud, trafficking in human beings, smuggling, drug trafficking, economic crime). Clearly, laundering through money remittance and currency exchange providers poses a number of regulatory and enforcement challenges. At the same time, there is low detection of money laundering in comparison to the size of the industry as a whole. In mitigation, money transmitters and currency exchanges are regulated and subject to on-site inspections.
Terrorist Financing Risk Assessment	
Threat	Terrorist groups use payment services to finance terrorist activities. They rely on IT skills to circumvent identification requirements and do not need specific knowledge to access this channel which is rather attractive and secure. The amounts concerned remain nevertheless quite limited.
Threat Score	3
Vulnerability	Although the risk exposure may be considered as quite high (significant level of transactions), the sector shows a good level of awareness to the risk vulnerability and is able to put in place the relevant red flags. The legal framework and controls are the basis of a good level of reporting.
Vuln. Score	2
	5
Money Laundering Risk Assessment	
Threat	Any use of P2P payment systems would be conducted through one established outside of Gibraltar.
Threat Score	1
Vulnerability	The risk exposure and the risk awareness of the sector are quite similar to what happens in the retails services sector. As far as the legal framework is concerned, it covers equally bank and payment institutions. Controls in place are nevertheless less efficient when dealing with payment institutions.
Vuln. Score	2
	3

Risk ID	15
Risk Name	Private banking-Deposits on accounts
Description	Perpetrators are using private banking and wealth management for investing in shares for integration of criminal proceeds, title of shares to conceal BO, frauds for predicate offence (e.g. insider dealing); brokerage accounts; investment to justify criminal proceeds as profit; predicate investment fraud. Placement of proceeds by using specialised, high-return financial services.
Terrorist Financing Risk Assessment	
Threat	The assessment of the TF threat related to private banking (wealth management) has not been considered as relevant. In that context, the TF threat is not part of the assessment.
Threat Score	1
Vulnerability	The assessment of the TF vulnerability related to private banking (wealth management) has not been considered as relevant. In that context, the TF vulnerability is not part of the assessment.
Vuln. Score	1
	2
Money Laundering Risk Assessment	
Threat	The assessment of the ML threat 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 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.
Threat Score	3
Vulnerability	Large amounts of transactions concerned and the fact that it implies high risk customers (PEPs) and potentially high risk areas (third countries with branches), the risk exposure is quite high. The low level of STRs shows that the controls in place are not necessarily adequate. However, there is a legal framework which establishes the basics of AML/CFT requirements.
Vuln. Score	3
	6

Risk ID	53
Risk Name	Sanctions
Description	That a Gibraltar transaction/structure is used to circumvent an international sanction.

Terrorist Financing Risk Assessment

Threat	A service provider may be unaware of applicable sanctions on a particular country and/or individual and may therefore agree to undertake or be a party to a transaction which contravenes an international sanction.
Threat Score	4
Vulnerability	Lack of centralised local list of applicable sanctions and local awareness.
Vuln. Score	2
	6

Money Laundering Risk Assessment

Threat	Not considered as present a ML risk
Threat Score	1
Vulnerability	Not considered as present a ML risk
Vuln. Score	1
	2

Risk ID	55
Risk Name	Proximity to Organised Crime
Description	Over the last few years there has been a marked increase in the rise of organised crime groups Organised Crime Groups (OCGs) operating in the area of Spain's Campo de Gibraltar. These groups have specialised in the importation of Hashish grown in Morocco into Europe, primarily using fast launches operating from nearby Spanish bases that are used to offload their cargo along the Spanish coastline. In more recent times there has been increased use by these OCG as conduits for the smuggling of cocaine from South America into Europe primarily via containers into the Spanish port of Algeciras for onwards distribution to the rest of Europe. Increasing influence by OCG in the Spanish regions is of concern as there are concerns regarding rule of law and their affluence has an ability to affect economic activity in the region. The concern for Gibraltar is that these groups may seek to establish business or economic activity in Gibraltar in order to launder the proceeds of the crimes committed in Spain.

Terrorist Financing Risk Assessment

Threat	There is no evidence to support a TF threat from this activity.
Threat Score	1
Vulnerability	There is no evidence to support a TF vulnerability from this activity, however, research suggests that there is a growing nexus between the proceeds of drugs trafficking in North Africa and TF.
Vuln. Score	1
	2

Money Laundering Risk Assessment

Threat	Criminals wishing to hide from law enforcement over the last three decades have become more sophisticated and mobile. An easily accessible frontier facilitates the movement of persons and therefore the ability to move illegitimate funds.
Threat Score	3
Vulnerability	The poor economic climate and unemployment rates in neighbouring regions are major contributory factors to the growth in illegal activity being conducted in the region which is exploiting the opportunities created by need. This in conjunction with cash rich businesses in Gibraltar being attractive mechanisms for OCG's to launder proceeds outside of the jurisdiction of their criminal activity. OCG's will target all aspects of the financial sector to achieve their ML aims and as such Gibraltar's well developed finance centre gives them opportunities to exploit. This is countered with the developed AML/CFT regimes throughout the financial sector.
Vuln. Score	3
	6

Total Risk Score	7
Risk ID	14
Risk Name	Corporate banking-Deposits on accounts
Description	Perpetrators use cash front businesses to inject proceeds into legal economy using company accounts with multi-signatories
Terrorist Financing Risk Assessment	
Threat	There is little evidence to suggest that Gibraltar has experienced any TF cases within the Banking sector to date. However, this is a common modus operandi for criminals to exploit.
Threat Score	1
Vulnerability	The banking industry in Gibraltar has a sound awareness of the TF risks posed and these are factored in to the FI's risk methodologies and assessments. Nonetheless, this sector has a high level of cash based transactions, making it more difficult to trace where payments originate from. The banking industry in Gibraltar is a small and long standing sector which has been regulated for many years.
Vuln. Score	1
	2
Money Laundering Risk Assessment	
Threat	Cash fronted businesses are an attractive modus operandi for criminals to exploit relative to ML schemes and will then be integrated into the banking system as a result.
	Gibraltar's regulation of the TCSP sector since the 1990s has ensured that the full AML/CFT regime has applied to this sector to the same standards as any FI. There is therefore a double control over corporate bank accounts applied at both FI and TCSP level to mitigate the threat. The differential in pricing of tobacco between Gibraltar and Spain and their unique geographical context results in OCG's exploiting this for the illicit trade in tobacco. This generates large volumes of cash in Gibraltar. With various retail sectors e.g. tobacco sellers, restaurants, beauty salons being able to generate and justify large volumes of cash this makes corporate banking attractive for ML activities.
Threat Score	3
Vulnerability	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 large number of corporates operating bank accounts in Gibraltar together with the number and variety of cash based businesses allows for a wider scope for ML activities to take place through corporate banking.
Vuln. Score	2
	5

Risk ID	12
Risk Name	Banking -Deposits on accounts
Description	Perpetrators are using institutional investors to invest in shares for integration of proceeds, title of shares to conceal beneficial ownership, frauds for predicate offence (e.g. insider dealing); brokerage accounts; investment to justify criminal proceeds as profit; predicate investment fraud. Placement of proceeds by using specialised, high-return financial services.

Terrorist Financing Risk Assessment

Threat	The assessment of the TF threat related to institutional investment- banks (securities, asset management, and investment) has been considered in conjunction with ML schemes related to institutional investment in order to hide the illegal origin of the funds. In that context, the TF threat does not benefit from a separate assessment.
Threat Score	2
Vulnerability	The assessment of the TF vulnerability related to institutional investment - banks (securities, asset management, and investment) has been considered in conjunction with ML schemes related to institutional investment. In that context, the TF vulnerability does not benefit from a separate assessment.
Vuln. Score	2
	4

Money Laundering Risk Assessment

Threat	Gibraltar has a well developed and mature KYC process including obtaining UBO data over many years of practice. This mitigates considerably the threat of these products being misused for ML.
Threat Score	1
Vulnerability	The risk exposure is inherently high due to the nature of the customer and the large amounts linked to the transactions. However, when provided by a bank, the investment service is quite well framed and controlled. The low level of STRs may be justified by the fact that due to the complexity of the transaction, few suspicious cases arose (in general, these transactions are approved by senior manager).
Vuln. Score	2
	3

Risk ID	48
Risk Name	Securities and Funds Sector
Description	Primary risk event That the funds and securities sector may be abused by investors to conceal ML or TF activities. Contributing risk events The securities sector is one of the core industries through which persons and entities can access the financial system, providing opportunities for criminals to misuse the financial system. The securities industry plays a key role in the global economy. Participants, globally, range from multinational financial conglomerates that employ tens of thousands of people to single-person offices offering stock brokerage or financial advisory services. The establishment of private funds and Experienced Investor Fund products locally could present an opportunity for ML and TF activities. In mitigation, the financial regulator has embarked on a series of workshops and interviews with all EIF Directors. The funds and securities sector in Gibraltar is nascent in relation to other territories.

Terrorist Financing Risk Assessment

Threat	Not considered at present a TF risk
Threat Score	0
Vulnerability	Not considered at present a TF risk
Vuln. Score	0
	0

Money Laundering Risk Assessment

Threat	Some of the features that have long characterised the securities industry, including its speed in executing transactions, its global reach, and its adaptability, can make it attractive to those who would abuse it for illicit purposes, including money laundering and terrorist financing due to the fact that the complexity of the structures and multiple relationships associated with funds can often give rise to particular difficulties and uncertainties with regards to the principle controller(s) and owner of the assets. Moreover, the securities sector is perhaps unique among industries in that it can be used both to launder illicit funds obtained elsewhere, and to generate illicit funds within the industry itself through fraudulent activities. Transactions and techniques associated with money laundering and the specific predicate securities offences are often difficult to distinguish.
Threat Score	4
Vulnerability	The risk lies in the creation of private funds which do not fall under the regulatory net.
Vuln. Score	3
	7

Risk ID	10
Risk Name	Payments in cash
Description	Perpetrators frequently need to use a significant portion of the cash that they have acquired to pay for the illicit goods they have sold, to purchase further consignments, or to pay the various expenses incurred in transporting the merchandise to where it is required. Despite the advantages and disadvantages of dealing in cash (detailed earlier in this report) for criminal groups, there is often little choice. The criminal economy is still overwhelmingly cash based. This means that, whether they like it or not, perpetrators selling some form of illicit product are likely to be paid in cash. The more successful the perpetrators are and the more of the commodity they sell, the more cash they will generate. This can cause perpetrators significant problems in using, storing and disposing of their proceeds. Yet despite these problems, cash is perceived to confer some significant benefits on them. In addition, the objective of criminals is to launder large amounts of cash, which are proceeds of criminal activity, by claiming that the funds originate from economic activities. They may launder amounts of cash, which are proceeds of criminal activity, by justifying its origin based on fictitious economic activities (both for goods and services). Terrorists may finance, through often small amounts of cash, terrorist activities without any traceability (see general description under cash intensive business).

Terrorist Financing Risk Assessment

Threat	The presence of a Schengen border with customs controls operating at all entry points together with added vigilance by HMC in relation to possible use of cash for tobacco purchasing makes this threat considerably reduced for Gibraltar.
Threat Score	1
Vulnerability	The presence of a Schengen border with customs controls operating at all entry points together with added vigilance by HMC in relation to possible use of cash for tobacco purchasing makes this threat considerably reduced for Gibraltar.
Vuln. Score	1
	2

Money Laundering Risk Assessment

Threat	Gibraltar has a very limited retail sector area, resulting in limited opportunities for criminals wishing to launder illicit funds. There are only approximately 255 businesses trading within the Main Street Area, being the main commercial district. Businesses are also deterred from accepting cash payments due to fees imposed by banks on the deposit of cash payments. The main threat for laundering would occur through criminal backed businesses which would act as fronts for the laundering of illicit funds.
Threat Score	3
Vulnerability	The definition of HVD's as a relevant financial business under POCA where they accept more than £8,000 in cash for transactions and the requirements to be regulated for the same by the OFT considerably reduces the vulnerability risk. The OFT has launched various outreach campaigns making HVD's aware of their obligations, reporting requirements, examples of suspicious activity and other relevant information which decrease our vulnerability further.
Vuln. Score	2
	5

Risk ID	45
Risk Name	Online gambling
Description	Online gambling could involve any product in the gambling sector or a combination of these. In addition to some of the risks identified for each sector offline, there may be additional risks associated with the lack of face-to-face contact enabled by the Internet. At the same time, electronic gambling offers an important mitigating feature in the possibility of tracking all transactions. A perpetrator uses gambling sites to deposit illicit funds and to request the pay out of winnings or unplayed balance. Legitimate online gambling accounts are credited with dirty funds (cashing in) followed by gambling on only small amount of funds, transferring the remaining funds to a different player (or to a different online gambling operator). The remaining funds are cashed out as if they were legitimate gambling earnings. Crime organisations may use several "smurfs" betting directly against each other using dirty funds. One of the "smurfs" will receive all the funds as an apparent winner, who will then cash out the funds as if they were legitimate gambling earnings. Crime organisations may purchase online casino accounts containing funds already uploaded by non-criminal players at a higher price than the real one. Crime organisations may also invent and bet on fictitious (non-existing) matches or events to ensure winnings.

Terrorist Financing Risk Assessment

Threat	The assessment of the TF threat related to online gambling has not been considered as relevant for the purpose of this first SNRA. In that context, the TF threat is not part of the assessment. In respect of online poker there is a potential threat of peer-to-peer transfers being used for the purposes of financing terrorism.
Threat Score	1
Vulnerability	The assessment of the TF threat related to online gambling has not been considered as relevant for the purpose of this first SNRA. In that context, the TF threat is not part of the assessment.
Vuln. Score	1
	2

Money Laundering Risk Assessment

Threat	In respect of online B2B operators, there is a need for them to remain vigilant in respect of the techniques which may be employed by money launderers, as they have oversight of the gambling activity which takes place on their games even though it is the B2C which ultimately bears the risk of ML by their customers. It is nevertheless required of B2Bs that they monitor activity which could be deemed suspicious and report it to the B2C. As acknowledged in the EU SNRA, the threat of remote operators being used for money laundering is in large part mitigated by the fact that transactions are so carefully recorded and monitored. The licensing regime ensures that only reputable operators with stringent standards in respect of AML processes and controls obtain licences. Online operators are regularly engaged by the Gambling Division in respect of AML issues, in particular upon the submission of SARs and onsite visits are conducted where it appears that there may be a gap or lack in respect of an operator's systems and controls.
Threat Score	3
Vulnerability	With a large number of transactions through this sector being low value/high volume, the majority of these transactions attract Customer Due Diligence measures in accordance with 4MLD

requirements and therefore could only be attractive to low value ML and TF risks.
As is the case for Financial Institutions the CDD measures increase substantially as the value of the transaction (bet or win) increases and come into play at £2000 value mark
Unlike other jurisdictions, Gibraltar has applied high entry standards for companies wishing to be awarded remote gambling licences. Operators are subject to a strong and independent regulator who is supported by a strong legislative framework.
The regulator has published its own Guidance Notes on AML/CFT controls and which all licensed operators have to comply with as part of their conditions of holding a licence.
Controls surrounding the establishment of new operators and changes in control of existing operators by the regulator mitigates the risk, to almost negligible, of abuse by criminal organisations of Gibraltar based operators.
This sector is advanced in its preparations for compliance with 4MLD.

Vuln. Score

2

5

Total Risk Score	6
Risk ID	30
Risk Name	Business activity of legal entities and legal arrangements
Description	EU Assessment Front companies used for fraud via false invoicing: Perpetrators use front company to apply false invoices to imported items, with the overpayments siphoned off to terrorist causes. Trade based money laundering: Perpetrators use Trade based money laundering (TBML) as a means of justifying the movement of criminal proceeds through banking channels (via letter of credit, invoices) or through the use of global transactions, often using false documents regarding the trade of goods and services. It can potentially allow the rapid transfer of large sums by justifying an alleged economic purpose. TBML schemes have also been used by international terrorist groups with complex funding methods . False loans: companies set up fictitious loans between them in order to create an information trail to justify transfers of funds of illegal origin. Perpetrators use fictitious loans as a mean for justifying movement of criminal proceeds through banking channels - without any economic reality. Gibraltar Assessment Gibraltar has a respected, regulated, well-established and important Trust and Corporate Service Providers (TCSP) sector. Gibraltar legal entities are commonly used both as asset holding, investment and transactions based vehicles for both the domestic as well international community. The same applies to corporate entities formed elsewhere but managed and/or controlled from within Gibraltar. All TCSPs are required to be licensed and are regulated by the Financial Services Commission. Gibraltar is fully up to date in meeting its international obligations in transparency and exchange of information and is fully compliant with European Union legislation.

Terrorist Financing Risk Assessment

Threat	On the basis of the elements gathered from law enforcement authorities and financial intelligence units, the level of TF threat related to business activities business activities of legal entities and legal arrangements is considered as moderately significant. There is little evidence to suggest that Gibraltar has experienced any TF cases within the TCSP sector to date. However, this is a common modus operandi for criminals to exploit.
Threat Score	1
Vulnerability	The TCSP industry in Gibraltar has a level of awareness of the TF risks posed and these are factored into its assessments. The TCSP industry in Gibraltar is a long standing sector which has been regulated for a significant number of years.
Vuln. Score	1
	2

Money Laundering Risk Assessment

Threat	This is an attractive modus operandi for criminals to exploit relative to ML schemes given it is fairly secure and the knowledge of expertise required is not significant. Gibraltar's regulation of the TCSP sector since the 1990s has ensured that the full AML/CFT regime has applied to this sector to the same standards as any FI. There is also a risk that an entity or individual could conduct unauthorised activity in accordance with the Financial Services (Investments and Fiduciary Services) Act 1989.
Threat Score	3
Vulnerability	Gibraltar has high requirements for AML/CFT as well as UBO identification measures. This decreases

the identified vulnerabilities.

Vuln. Score

1

4

Risk ID	7
Risk Name	Cash couriers / cross external border cash movements
Description	This risk scenario is intrinsically linked to use of/payment in cash and to high value denomination banknotes risk scenario. Criminals or terrorist financiers who generate/accumulate cash proceeds seek to aggregate and move these profits from their source, either to repatriate funds or to move them to locations where one has easier access to placement in the legal economy. The characteristics of such locations are a predominant use of cash, more lax supervision of the financial system or stronger bank secrecy regulations. It may also be used by terrorists to transfer rapidly and safely funds from one location to another, including by using cash concealed in air transit. Cash couriers may use air, sea or rail transport to cross an EU external border. In addition, cash may be moved across external borders unaccompanied such as in containerised or other forms of cargo, or concealed in mail or post parcels. If perpetrators wish to move very large amounts of cash, often a valuable option is to conceal it in cargo that can be containerised or otherwise transported across borders. Perpetrators may also use sophisticated concealment methods of cash within goods which are either carried across the external border by a courier or are sent by regular mail or post parcel services. Although unaccompanied consignments tend to be smaller than those secreted within vehicles, or on the person of cash couriers, the use of high denomination banknotes can still result in seizures of significant value.

Terrorist Financing Risk Assessment

Threat	With no terrorist groups known or suspecting to be operating in Gibraltar and the strict border controls already in operation between Gib/Spain land border and the infrequent ferry crossing to Morocco, this threat is considered to be much reduced.
Threat Score	1
Vulnerability	Strict controls at entry points which are subject to Schengen requirements make this unlikely.
Vuln. Score	1
	2

Money Laundering Risk Assessment

Threat	Use of cash for the purchase of tobacco could be used to hide proceeds of crimes. 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. This added to the fact that OCG's in close proximity to Gibraltar, working in illicit tobacco activity, are also active in drugs trafficking which creates further high cash volumes.
Threat Score	2
Vulnerability	HM Customs have proactive monitoring of entry points and intercept cash importations. This is coupled with a cash declaration process for entry and exit from EU. Cash confiscation stats may indicate relatively small amounts of cash are imported for tobacco purchasing, however this maybe a result of other factors such as difficulty in detection, the non-requirement to make declarations between EU borders, the limited time frame in which POCA powers of seizure have been used. The majority of cash seizures that have been made relate to the illicit tobacco trade. Levels of unemployment in surrounding area's of Spain increase the attractiveness of criminality and the profitability of OCG's.

Gibraltar’s relative affluence compared to its neighbouring Spanish towns makes it a more attractive place to launder cash through cash based businesses.

Vuln. Score

2
4



Risk ID	54
Risk Name	Tobacco
Description	That the monies generated by tobacco sales presents an attractive target for money launderers.
Terrorist Financing Risk Assessment	
Threat	Not considered at present a TF risk
Threat Score	0
Vulnerability	Not considered at present a TF risk
Vuln. Score	0
	0

Money Laundering Risk Assessment

Threat	Gibraltar's tobacco wholesale and retailing businesses generates an important volume of cash sales as most of the retail operations are made in a cash only environment from visitors to Gibraltar. When most of this cash is generated in Euros in a Sterling zone there is then the issue of currency conversion to also consider. The ability to justify large volumes of cash to FI's makes this an attractive opportunity for OCG's both locally and from surrounding areas to exploit to launder the proceeds of illicit tobacco activity as well as other crimes.
Threat Score	3
Vulnerability	There appears to be no evidence to suggest that tobacco sales present significant opportunities to launder the cash through the system or that this is being exploited by ML or TF operations other than in a small and opportunistic scale. Turnover from legitimate tobacco sales by both wholesalers and retailers are sufficiently large that the laundering of large volumes of cash would raise little suspicions with FI's. The highest sub-risk identified is in the possible use of licensed wholesale and retail operations to obfuscate cash deposits.
Vuln. Score	3
	6

Risk ID	42
Risk Name	Gaming machines (outside casinos)
Description	A perpetrator deposits illicit funds (cash) into gaming machines or uses it to purchase tokens for the machines. Certain gaming machines also allow only a small part of the (deposited) amount to be staked, then requests the pay out of the remaining funds into a bank account or in cash with a receipt (thereby providing opportunities for legitimizing a larger sum than actually gambled). A perpetrator uses electronic roulette to launder money placing even bets on both red and black, as well as a smaller stake on 0; the vast majority of the stake will never be lost as this is a 50/50 stake and there will be receipts confirming the winnings. Moreover, Ticket In Ticket Out (TITO) vouchers from machines in casinos, arcades or betting shops can be used for money laundering and cashed in at a later date or by third parties. A perpetrator can do all this repeatedly and/or in multiple venues to minimize suspicions or bypass limits on stakes or playtime.

Terrorist Financing Risk Assessment

Threat	The assessment of the TF threat related to gaming machines has not been considered as relevant. In that context, the TF threat is not part of the assessment.
Threat Score	1
Vulnerability	The assessment of the TF vulnerability related to gaming machines has not been considered as relevant. In that context, the TF vulnerability is not part of the assessment.
Vuln. Score	1
	2

Money Laundering Risk Assessment

Threat	The licensing of gaming machines outside casinos was brought into the Gambling Division's remit as from 1 April 2016. Both suppliers of gaming machines and businesses which keep gaming machines on their premises must apply for a licence.
Threat Score	2
Vulnerability	Although there is some degree of regulatory oversight in respect of gaming machines, this has been hampered by the absence of a full time regulator for land-based gambling, who would deal with AML/CFT issues as they pertain to gaming machine suppliers and premises.
Vuln. Score	2
	4

Risk ID	41
Risk Name	Casinos
Description	A perpetrator purchases chips at the casino at a dedicated point of sale (for cash or anonymous pre-paid cards) and these chips can be used when playing on a wide variety of games (with clearly defined rules). Casino staff (croupiers) interacts with players in well regulated games such as Baccarat roulette, black-jack and many more. If winning, the player receive chips at the table, which then have to be converted back to cash at a dedicated point of sale (whereby legitimising illicit funds). A perpetrator could use 'mules' or collaborators that buy chips on his behalf for illicit cash and the main perpetrator will receive the chips in the casino – and exchanging the chips to cash pretending that he won these in the games offered at the casino. A perpetrator could also take advantages from the fact that certain casino games provide for a high return on stakes (depending on high/low risk bets). Two players may also cooperate and place bets on a roulette table on red and black at the same time with only a 3% chance of losing their accumulated stakes. A perpetrator may also transfers funds from one casino to another (if legally allowed), giving access to chips to another player. In such cases, casinos are used like financial institutions through accounts to accounts transfers of funds.

Terrorist Financing Risk Assessment

Threat	The assessment of the TF threat related to casinos has not been considered as particularly relevant. In that context, the TF threat is not part of the assessment.
Threat Score	1
Vulnerability	The assessment of the TF vulnerability related to casinos has not been considered as relevant. In that context, the TF vulnerability is not part of the assessment.
Vuln. Score	1
	2

Money Laundering Risk Assessment

Threat	There are two land-based casinos currently licensed. They fall under the remit of the Gambling Division, however, our engagement with them on AML/CFT issues has been somewhat limited in comparison to online operators. The Gambling Division is in the process of producing a separate AML Code specifically for land-based operators. No SARs have been submitted by either casino. In part this is likely to be due to the level of controls in place, however, further engagement is required with the land-based sector.
Threat Score	2
Vulnerability	Gaming operators are relevant financial services business for AML/CFT purposes and are supervised as such by the Gambling Division.
Vuln. Score	2
	4

Total Risk Score	5
Risk ID	47
Risk Name	Tax Planning Structures and Transactions
Description	That by the misuse of tax planning, structures and shielding the real purpose of any structure, evasion may take place or it is used to conceal actual proceeds of crime.
Terrorist Financing Risk Assessment	
Threat	Not considered at present a TF risk
Threat Score	0
Vulnerability	Not considered at present a TF risk
Vuln. Score	0
	0
Money Laundering Risk Assessment	
Threat	Abuse of corporate and legal structures, abuse of nominee shareholdings, corporate directors and banking facilities for the same. However, tax evasion is a serious criminal offence and a predicate offence for the purposes of money laundering and professionals are aware that suspicious activity in this area is reportable.
Threat Score	3
Vulnerability	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.
Vuln. Score	2
	5

Risk ID	16
Risk Name	Crowdfunding
Description	Perpetrators can create platforms to collect/accumulate funds and transfers them abroad for ML purposes or to finance terrorist attacks. This can be done by creating crowdfunding platforms directly linked to financial institutions or left to private initiatives on the internet. Crowdfunding platforms are set up under fictitious projects in order to allow collection of funds which are then withdrawn within the EU or transferred abroad. This could be used either to collect funds from legitimate sources for the purpose of terrorist financing – or to collect illicit funds from criminal activities using anonymous products. Perpetrators post messages on the internet asking for donations in the form of prepaid mobile phone cards which are sold to raise funds; direct requests on Internet (via Tweeter) for specific amounts used ultimately for the purchase of illicit products. Social media misuses (the so called "crowdsourcing") are another kind of risk scenario. Terrorists groups in particular have made use of social media and other online and mobile platforms to obtain funds which are channelled afterwards through different means of payment. This type of crowdsourcing is not further analysed in this fiche.

Terrorist Financing Risk Assessment

Threat	Gibraltar agrees with the EU TF threat assessment. However, we have not encountered any cases in the jurisdiction where criminals have exploited this modus operandi for TF purposes.
Threat Score	1
Vulnerability	There is currently no harmonised structure in this sector, however, there are various instances where the activities conducted will fall under other legislation and supervisory framework. Furthermore, there has been no indication that perpetrators intend to use this method for criminal purposes which decreases the vulnerability to this risk.
Vuln. Score	1
	2

Money Laundering Risk Assessment

Threat	Gibraltar agrees with the EU ML threat assessment. Moreover, we have not encountered any cases in the jurisdiction where criminals have exploited this modus operandi for ML purposes.
Threat Score	2
Vulnerability	Although large sums could be handled within this area, the risk exposure is rather limited in Gibraltar given there has been little interest to pursue crowdfunding activities. There is currently no harmonised structure in this sector, however, there are various instances where the activities conducted will fall under another legislation and supervisory framework. Furthermore, there has been no indication that perpetrators intend to use this method for criminal purposes which decreases the vulnerability to this risk.
Vuln. Score	1
	3

Risk ID	39
Risk Name	Betting
Description	Three basic scenarios have been identified: (1)a perpetrator places a bet and cashes in the winnings (conversion); (2)a perpetrator deposits cash into their betting account and withdraws it after a period of time without actually staking it (concealment); (3)a perpetrator places money in a betting account in one location and an accomplice withdraws the funds in another location (concealment, disguise and transfer). A perpetrator can increase their odds of winning by placing bets on a series of events which will give more favourable accumulated odds -or reduce the risk of losing by hedging bets (i.e. betting on both possible outcomes of the same event). A perpetrator can also remove any uncertainty altogether by approaching a winner and purchasing the winning betting slip.

Terrorist Financing Risk Assessment

Threat	The assessment of the TF threat related to betting activities has not been considered as relevant. In that context, the TF threat is not part of the assessment.
Threat Score	1
Vulnerability	The assessment of the TF vulnerability related to betting activities has not been considered as relevant. In that context, the TF threat is not part of the assessment.
Vuln. Score	1
	2

Money Laundering Risk Assessment

Threat	Gibraltar has a highly regulated gambling sector covering all aspects of gambling. This regulation mitigates the identified risks considerably.
Threat Score	2
Vulnerability	There is currently only one betting shop which is licensed and regulated by the Gambling Division. This licence was awarded to a longstanding and experienced licensee. The licensing process any new applicants must undergo with the Gambling Division greatly reduces the risks of infiltration and ownership of a betting shop which is deemed to be the predominant AML threat by the EU SNRA. Betting shops are relevant businesses under POCA and are a licensable entity under the Gambling Act. They are supervised by the Gambling Division for AML/CFT purposes. Separate AML guidance for the land-based gambling sector will be developed to provide the current betting shop and any future shops with clearer guidance on the potential risks and how to mitigate them.
Vuln. Score	1
	3

Risk ID	46
Risk Name	Collect and transfers of funds through a Non-Profit Organisation (NPO)
Description	Establishment of NPOs to "fund raise" whereby criminals funds are gradually sent to the NPOs: -complicit NPOs may intentionally support a terrorist group or a criminal organisation -legitimate NPOs may be exploited by "outsiders" - legitimate NPOs may be exploited by "insiders". • 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 -complicit NPOs may intentionally support a terrorist group or a criminal organisation -legitimate NPOs may be exploited by "outsiders" - legitimate NPOs may be exploited by "insiders".

Terrorist Financing Risk Assessment

Threat	Gibraltar has a regulated Charities and Friendly Societies sector which has been the subject of a separate national risk assessment process. This has not identified weaknesses nor evidence of the use of the same for TF purposes.
Threat Score	2
Vulnerability	Reporting and accountability, particularly in the Charities sector ensures oversight to prevent TF risks from materialising.
Vuln. Score	1
	3

Money Laundering Risk Assessment

Threat	Gibraltar has a regulated Charities and Friendly Societies sector which includes reviews of financial statements etc. The high level of transparency over the financial affairs of the charities sector minimises the threat considerably.
Threat Score	1
Vulnerability	Reporting and accountability, particularly in the Charities sector ensures oversight to prevent ML risks from materialising.
Vuln. Score	1
	2

Risk ID	13
Risk Name	Brokers - Deposits on Account
Description	Perpetrators are using institutional investors to invest in shares for integration of proceeds, title of shares to conceal BO, frauds for predicate offence (e.g. insider dealing); brokerage accounts; investment to justify criminal proceeds as profit; predicate investment fraud. Placement of proceeds by using specialised, high-return financial services.

Terrorist Financing Risk Assessment

Threat	There is a very limited securities brokerage market in Gibraltar which in any case offers very simple and narrow product range making this relatively unattractive for TF purposes.
Threat Score	2
Vulnerability	There is a very limited securities brokerage market in Gibraltar which in any case offers very simple and narrow product range making this relatively unattractive for TF purposes.
Vuln. Score	1
	3

Money Laundering Risk Assessment

Threat	There is a very limited securities brokerage market in Gibraltar which in any case offers very simple and narrow product range making this relatively unattractive for ML purposes where any large amount would soon show up as unusual.
Threat Score	1
Vulnerability	This sector is undeveloped in Gibraltar and unlikely to be used for any large amounts.
Vuln. Score	1
	2

Risk ID	28
Risk Name	Safe custody services
Description	Perpetrators rent multiple safe custody services (commercial or banking ones) to store large amounts of currency, monetary instruments, or high-value assets awaiting conversion to currency, for placement into the banking system. Similarly, a perpetrator establishes multiple safe custody accounts to park large amounts of securities awaiting sale and conversion into currency, monetary instruments, outgoing funds transfers, or a combination thereof, for placement into the banking system. Free zones may be used as shelter for illicit activities including proceeds from criminal activities.

Terrorist Financing Risk Assessment

Threat	The assessment of the TF threat related to safe custody services has not been considered as relevant. In that context, the TF threat is not part of the assessment.
Threat Score	1
Vulnerability	The assessment of the TF vulnerability related to safe custody services has not been considered as particularly relevant. In that context, the TF vulnerability is not part of the assessment.
Vuln. Score	1
	2

Money Laundering Risk Assessment

Threat	There are no Safe Custody services offered in Gibraltar.
Threat Score	1
Vulnerability	When provided by credit and financial institutions, safe custody services are subject to CDD requirements and controls. However, it is not always possible to understand exactly the source of funds and ongoing monitoring may have a blind spot since the content is usually unknown to the financial institution. In addition, these safe deposits may be accessible to third parties other than the initial customer which increases the vulnerability. The market is fragmented with the emergence of private entities and other commercial storage/safe services.
Vuln. Score	2
	3

Risk ID	37
Risk Name	Services from accountants, auditors, tax advisors
Description	Perpetrators may employ or require the services of accountants, auditors or tax advisors with a more or less level of involvement of the accountant, auditor or tax advisor himself with the aim to: -misuse client accounts, -purchase of real property, -creation of trusts and companies/ management of trusts and companies, -undertaking certain litigation, setting up and managing charities -over or under-invoicing or false declaration around import/export goods. -providing assurance -tax compliance They may be involved in ML schemes through the creation of 'opaque structures' defined as business structures where the true identity of the owner(s) of entities and arrangements in that structure is concealed through the use of, for example, nominee directors. The creation of such structure often set up in multiple jurisdictions including offshore centres is complicated and requires both regulatory and tax services of professionals.

Terrorist Financing Risk Assessment

Threat	Gibraltar has not experienced any TF cases within this sector to date. Therefore, there is no indication that criminals have the intention to use this modus operandi.
Threat Score	1
Vulnerability	The assessment of the TF vulnerability related to services from accountants, auditors, tax advisors has been considered in conjunction with ML schemes related to services from accountants, auditors, tax advisors in order to hide the illegal origin of the funds. In that context, the TF threat does not benefit from a separate assessment. However the complexities of setting up and running systems through these methods and the increased CDD that would be associated with them compared to other simpler methods of TF and ML reduces the threat and vulnerability in this area. Additionally, there is little evidence to show that this method of business is exploited for TF purposes.
Vuln. Score	1
	2

Money Laundering Risk Assessment

Threat	Services from tax advisors/auditors/accountants are recurrently used in ML schemes, are considered as easily accessible and seen by organised crime organisations as a way to compensate their lack of expertise. Gibraltar markets itself as a tax efficient jurisdiction which makes it attractive to those from other jurisdictions seeking opportunities to misuse its services. Gibraltar has not experienced any ML cases within this sector to date. Therefore, there is no indication that criminals have the intention to use this modus operandi.
Threat Score	2
Vulnerability	This sector requires knowledge and planning expertise which makes it unattractive. Furthermore, this sector has a low level of cash based and anonymous transactions. Additionally, Gibraltar has recently implemented the UBO reporting requirements where a register is held evidencing the identification of the UBOs behind every company incorporated in Gibraltar. There is little evidence to show that this method of business is exploited for ML purposes.

Auditors are themselves relevant financial businesses under POCA and the conduct of TCSP work by this sector would also define them as TCSPs and require authorisation as well being subjected to the full POCA regime.

Vuln. Score

1

3

Risk ID	9
Risk Name	High value banknotes
Description	In spite of steady growth in non-cash payment methods and a moderate decline in the use of cash for payments, the total value of euro banknotes in circulation continues to rise year-on year beyond the rate of inflation. Cash is largely used for low value payments and its use for transaction purposes is estimated to account for around one-third of banknotes in circulation. Meanwhile the demand for high denomination notes, such as the EUR 500 note, not commonly associated with payments, has been sustained. These are anomalies which may be linked to criminal activity. Perpetrators use high value denominations, such as EUR 500 banknotes, to make the cash transportation easier (the larger the denomination, the more funds can be shrunk to take up less space).

Terrorist Financing Risk Assessment

Threat	The assessment of the TF threat related to high value denomination banknotes shows that terrorist groups are not really keen in using high value denominations. They are not necessarily easy to access and, given that they can be detected quite easily they are not attractive for terrorist groups whose first objective is to get cash as quickly as possible. For sake of discretion, terrorist groups tend to favour low denominations banknotes. LEAs have detected few cases which tend to demonstrate that the intent and capability are not really significant
Threat Score	2
Vulnerability	Nearly all Gibraltar based business and all financial sector firms do not accept high-value EURO denomination notes (200 and 500). Largest Sterling note in circulation in Gibraltar is the £100 note.
Vuln. Score	1
	3

Money Laundering Risk Assessment

Threat	Nearly all Gibraltar based business and all financial sector firms do not accept high-value EURO denomination notes (200 and 500). Largest Sterling note in circulation in Gibraltar is the £100 note.
Threat Score	1
Vulnerability	It is an unlikely scenario to have high denomination bank notes being used in Gibraltar.
Vuln. Score	1
	2

Risk ID	56
Risk Name	Football Leagues
Description	Use of local football clubs being used to launder proceeds of crime through ownership or control by persons connected with criminal activity.

Terrorist Financing Risk Assessment

Threat The TF risk is not considered to be significant for this risk.

Threat Score 0

Vulnerability The TF risk is not considered to be significant for this risk

Vuln. Score 0

0

Money Laundering Risk Assessment

Threat Possible existing connections between owners and directors of clubs and criminal activity/illegal tobacco smuggling.

Threat Score 3

Vulnerability Recent cash injections into the football scene through UEFA and FIFA membership and professionalism of the sport are creating opportunities for cash and other donations to be used as fronts for placements of criminal proceeds.

Vuln. Score 2

5

Risk ID	32
Risk Name	High value goods – artefacts and antiquities
Description	Terrorist financing - Perpetrators earn revenue from the sale of looted artefacts and antiquities. The trafficking in cultural goods is among the biggest criminal trades, estimated to be the third or fourth largest, and despite the fact that there are hardly any instruments for measuring this trade or any data on illicit commerce. It is estimated that only 30-40% of antique dealings take place through auction houses where the pieces are published in catalogues; the rest occur through private transactions. On the whole, the total financial value of the antiquities market ranks third after drug and arms trafficking and amounts to up to \$6 billion yearly. Money laundering – Perpetrators convert proceeds of criminal activities into antiques and art goods to store or move these assets more easily. Threat

Terrorist Financing Risk Assessment

Threat	At this stage, there is limited/no evidence that such scenario is used to finance terrorist activities in the EU. However, it represents an attractive source of revenue for organisations controlling territory in conflict zones, which could then be used to finance terrorist activities in the EU. Nevertheless, the level of knowledge, expertise and planning capabilities required reduces the level of threat. But lack of any evidence to support this occurring in Gibraltar leads us to have a lower score.
Threat Score	1
Vulnerability	High Value Goods dealers are defined as relevant financial business in POCA and as such are required to implement AML/CFT measures. HVGs are subject to on-site verification by the OFT.
Vuln. Score	1
	2

Money Laundering Risk Assessment

Threat	This risk scenario may represent an attractive tool to convert proceeds of crime in clean cash. However, it requires high level of expertise and is not really secure for organised crime organisations.
Threat Score	2
Vulnerability	High Value Goods dealers are defined as relevant financial business in POCA and as such are required to implement AML/CFT measures. HVGs are subject to on-site verification by the OFT. There is very little business conducted in Gibraltar with artefacts and antiquities.
Vuln. Score	1
	3

Total Risk Score	4
Risk ID	44
Risk Name	Poker (land-based/offline)
Description	A perpetrator purchases chips at the casino (or at the relevant licenced premises) at a dedicated point of sale (for cash or anonymous pre-paid cards) and these chips may be transferred to another player through deliberate losses (fold on a winning hand to ensure that the accomplice receive the chips). Chips are converted into cash or transferred in another way to the customer. A perpetrator (organised crime organisations) may also seek to infiltrate the organisational structure of the licenced premises where poker games or tournaments are organised (e.g. casinos or private clubs) or directly or indirectly apply for a licence to organise a poker tournament, which may be open or on invitation only.
Terrorist Financing Risk Assessment	
Threat	The assessment of the TF threat related to poker has not been considered as relevant. In that context, the TF threat is not part of the assessment.
Threat Score	1
Vulnerability	The assessment of the TF threat related to poker has not been considered as relevant. In that context, the TF threat is not part of the assessment.
Vuln. Score	1
	2
Money Laundering Risk Assessment	
Threat	Poker events take place at the licensed casinos and the Gambling Division is informed beforehand of the arrangements in order to ensure that the poker events are adequately supervised. Smaller poker events held by clubs and associations require prior approval by the Gambling Division although these are rare and are not held for the purposes of commercial gain.
Threat Score	1
Vulnerability	The land-based casinos, of which there are two, have undergone a stringent licensing process to ensure their suitability and are regulated by the Gambling Division.
Vuln. Score	1
	2

Risk ID	43
Risk Name	Lotteries
Description	The relatively low return to players makes direct purchase of lottery tickets a costly and unattractive form of money laundering. Direct purchase of lottery tickets to win a prize is therefore not considered a likely risk scenario. On the contrary, the modus operandi of purchasing a winning ticket - a perpetrator purchases a lottery ticket from the winner (possibly through collusion with the sales agent) and cashes the prize with a receipt is more viable scenario reported by LEAs.

Terrorist Financing Risk Assessment

Threat	The assessment of the TF threat related to lotteries has not been considered as relevant. In that context, the TF threat is not part of the assessment.
Threat Score	1
Vulnerability	The assessment of the TF vulnerability related to lotteries has not been considered as relevant. In that context, the TF threat is not part of the assessment.
Vuln. Score	1
	2

Money Laundering Risk Assessment

Threat	Lotteries, other than the state-run National lottery, tend to be small, club or charity based, and it is accepted that the primary purpose of participation is to contribute to the 'good cause' in question. Associations nevertheless are required to request permission from the Gambling Division which helps to reduce any vulnerabilities in respect of the already negligible ML threat. The National Lottery is run by the Treasury Department.
Threat Score	1
Vulnerability	Based on the vulnerability assessment, it appears that lotteries as such are not a viable risk scenario but that the risks are more related to (purchasing of) winning tickets. Although lottery operators are currently not considered as obliged entities in the whole EU, national frameworks in place have introduced control and identification measures, in particular relating to high winnings. Still, the (purchasing of) winning tickets risk scenario remains an important point of concern.
Vuln. Score	1
	2

Risk ID	52
Risk Name	Bribery & Corruption
Description	That businesses and public sector bodies may be obtaining or granting contracts and/or business on the basis of corrupt business practices or bribery.

Terrorist Financing Risk Assessment

Threat	Not considered at present a TF risk
Threat Score	0
Vulnerability	Not considered at present a TF risk
Vuln. Score	0
	0

Money Laundering Risk Assessment

Threat	Lack of awareness, by some, of the provisions of the Crimes Act which criminalises bribery and corruption, the OECD Convention relating to bribery of officials that was extended to Gibraltar as well as the extra-territorial provisions of the UK Bribery Act that extend to British Citizens. OCG's both in Gibraltar and in the surrounding areas generate significant amounts of illegitimate cash. This can be laundered through cash based businesses in Gibraltar. This exposes local government officials to bribery in terms of the issuing of business licences, contracts etc. Gibraltar's well developed TSCP and legal sectors are attractive to major international clients including PEP's which exposes.
Threat Score	2
Vulnerability	The proximity to countries where such practices are commonplace and which may wish to use Gibraltar-based products to conceal the receipts of the bribery or corruption. Gibraltar's TSCP sector is vulnerable to the setting up of corporate structures under false pretences in order to facilitate the laundering of the proceeds of major international bribery and corruption. An absence of standard reporting procedures and closeness of the local community may hinder the exposure of local cases of bribery and corruption.
Vuln. Score	2
	4

Risk ID	31
Risk Name	Termination of legal entities and legal arrangements
Description	Fraud using bankruptcy/judicial liquidation of a company: following the bankruptcy of a company, the same company is bought by a former shareholder who creates a new structure to pursue the same business activity without financial difficulties anymore. Perpetrators cash out funds from the front company before the illegal activities are detected or before assets are seized by competent authorities.

Terrorist Financing Risk Assessment

Threat	The assessment of the TF threat related to termination of business activity has been considered in conjunction with ML schemes related to termination of business activity in order to hide the illegal origin of the funds. In that context, the TF threat does not benefit from a separate assessment.
Threat Score	1
Vulnerability	The assessment of the TF vulnerabilities related to termination of business activity has been considered in conjunction with ML schemes related to termination of business activity in order to hide the illegal origin of the funds. In that context, the TF threat does not benefit from a separate assessment. Furthermore, there is no evidence that these scenarios have been previously encountered in Gibraltar.
Vuln. Score	1
	2

Money Laundering Risk Assessment

Threat	On the basis of the elements gathered during the assessment phase, the level of ML threat related to termination of business activity is considered as lowly/moderately significant.
Threat Score	1
Vulnerability	While bankruptcy is an issue for some Member States, the detection of such cases and the level awareness of the sector and other obliged entities allow considering that the level of vulnerability is lowly/moderately significant. Furthermore, there is no evidence that these scenarios have been previously encountered in Gibraltar.
Vuln. Score	1
	2

Risk ID	40
Risk Name	Bingo
Description	A perpetrator purchases cards - traditionally with cash - on which a random series of numbers are printed. Players mark off numbers on their cards which are randomly drawn by a caller (employed by the gambling operator), the winner being the first person to mark off all their numbers. A winning card could be purchased for a higher amount, like a lottery ticket or betting slip.

Terrorist Financing Risk Assessment

Threat	The assessment of the TF threat related to bingo has not been considered as relevant. In that context, the TF threat is not part of the assessment.
Threat Score	1
Vulnerability	The assessment of the TF vulnerability related to bingo has not been considered as relevant. In that context, the TF threat is not part of the assessment.
Vuln. Score	1
	2

Money Laundering Risk Assessment

Threat	Gibraltar has a highly regulated gambling sector covering all aspects of gambling including Bingo. This regulation mitigates the identified risks considerably.
Threat Score	1
Vulnerability	Bingo takes place in the licensed land-based casinos and therefore falls under the licensing and regulatory remit of the Gambling Division. Smaller clubs and associations may hold bingo events but these are small-scale and for charitable purposes.
	There is negligible risk of ML in this area.
Vuln. Score	1
	2

Risk ID	23
Risk Name	Business loans
Description	Perpetrators repay business loans with criminal funds (including use of the credit card for repayments in order to legitimise sources of funds). Loans provide legitimacy to criminal funds.

Terrorist Financing Risk Assessment

Threat	The assessment of the TF threat related to business loans shows that there few cases where terrorist organisations have used this scenario to collect funds. Business loans are not easily accessible to terrorist organisations because they do not fulfil the conditions to subscribe to this kind of products (level of salary too low, origins of funds coming from social benefits). There are also few cases where sanctioned entities (listed organisations) may try to use business loans to finance terrorist activities through shell companies. However, it requires a sophisticated level of expertise and knowledge.
Threat Score	1
Vulnerability	The assessment of the TF vulnerability related to business loans has been considered in conjunction with ML schemes related to business loans. In that context, the TF vulnerability does not benefit from a separate assessment.
Vuln. Score	1
	2

Money Laundering Risk Assessment

Threat	The assessment of the ML threat related to business loans shows that there are few indicators that criminals have the intention to exploit this risk scenario which is perceived as unattractive. Fake loans are most of the time part of fraud schemes (e.g. 2 companies subscribe to a fake loan and use a bank to process the transfer of funds) but are not necessarily use to launder proceeds of crime.
Threat Score	1
Vulnerability	The level of ML vulnerability is considered as lowly significant
Vuln. Score	1
	2

Risk ID	24
Risk Name	Consumer credit and low value loans
Description	Terrorists/organised crime groups use "payday", consumer credit or student loans (short-term, low value but high interest) to fund plots. Loans are given for relatively low amounts allowing the access to funds, the sources for which are untraceable as long as the money is not transferred. Terrorists/organised crime groups use cash withdrawals with credit cards: criminals withdraw cash with their own credit cards on an ATM, generating a negative balance on their accounts. They disappear with the funds without any intention to reimburse this "forced" credit.

Terrorist Financing Risk Assessment

Threat	The credit market in Gibraltar is very specific and has a narrow use which would make this product highly unlikely for TF purposes. There is no evidence to suggest that this modus operandi has been exploited for TF cases.
Threat Score	1
Vulnerability	In Gibraltar, credit may only be granted by licensed and regulated entities, all of whom are considered to be relevant financial businesses and are subject to the POCA requirements.
Vuln. Score	1
	2

Money Laundering Risk Assessment

Threat	The assessment of the ML threat related to low value loans has not been considered as particularly relevant. In that context, the ML threat is not part of the assessment. There is no evidence to suggest that this modus operandi has been exploited for ML cases.
Threat Score	1
Vulnerability	The assessment of the ML vulnerability related to low value loans has not been considered as particularly relevant. In that context, the ML threat is not part of the assessment. In addition and according to the data collected from firms, loans are only being provided to entities and individuals within Gibraltar. Firms are also not allowed to passport their services to other EU states.
Vuln. Score	1
	2

Risk ID	25
Risk Name	Mortgage credit and high value asset-backed credits
Description	In the case of money laundering, perpetrators disguise and invest proceeds of crime by way of real estate investment. Proceeds of crime are used for deposit, repayments and early repayment of asset. In the case of terrorist financing, perpetrators use high value assets backed credit/mortgage loans (medium/long-term, high value with low interest) to fund plots. Loans are subscribed for relative high amounts to access funds which are untraceable as long as the money is not transferred.
Terrorist Financing Risk Assessment	
Threat	Mortgage credit requires a high level of knowledge and expertise to understand the product and to provide the relevant documentation (forged documents). It is not attractive due to the fact that it implies the complicity of a third party, beneficiary of the funds. There are no stand-alone mortgage credit or high value asset-backed credit firms, only those which are licensed to do so under its Banking licence within its wider permissions and are regulated accordingly.
Threat Score	1
Vulnerability	The assessment of the TF vulnerability related to mortgage credit shows that this product is not vulnerable to TF risks because few or even no cases were found by LEAs. The risk awareness of the sector is quite low but this does not mean that the risk is unknown, but that it is unlikely and that red flags are adequate in case of suspicion of fraud. There has not been any interest in this area, therefore, it is not considered to be a sector which is going to grow and potentially be a risk for the jurisdiction.
Vuln. Score	1
	2

Money Laundering Risk Assessment

Threat	In the ML context, mortgage credit is a vehicle favoured by criminal organisations. It allows hiding the volume of assets and the beneficial ownership. It requires a moderate level of expertise. Gibraltar recognises that this is a modus operandi which is often exploited by criminals, however, there is no evidence to show that this has been done in Gibraltar to date. There are no stand-alone mortgage credit or high value asset-backed credit firms, only those which are licensed to do so under its Banking licence within its wider permissions and are regulated accordingly.
Threat Score	1
Vulnerability	When provided by banks, mortgage credit products are as vulnerable as retail banking. However, most of the time, the interaction with the real estate sector makes the vulnerabilities higher. There has not been any interest in this area, therefore, it is not considered to be a sector which is going to grow and potentially be a risk for the jurisdiction.
Vuln. Score	1
	2

Risk ID	26
Risk Name	Life-Insurance
Description	Perpetrators are using fraud to life insurance products to fund their activities. Early redemption life policies to receive lump sums, particularly where product can be transferred. Money laundering and terrorist financing risks in the insurance industry may be found in life insurance and annuity products. Such products allow a customer to place funds into the financial system and potentially disguise their criminal origin or to finance illegal activities. Relevant risk scenarios are typically focussed on investment products in life insurance (and not on death benefit products as such).

Terrorist Financing Risk Assessment

Threat	Gibraltar has not experienced any TF cases within the Life Insurance sector to date. Therefore, there is no indication that criminals have the intention to use this modus operandi.
Threat Score	1
Vulnerability	This sector requires knowledge and planning expertise which makes it unattractive. Furthermore, given the nature of the business and activity, it is expected to include a low level of cash based and anonymous transactions. The life insurance industry in Gibraltar is a small and long standing sector which has been regulated for many years.
Vuln. Score	1
	2

Money Laundering Risk Assessment

Threat	Gibraltar has not experienced any ML cases within the Life Insurance sector to date. Therefore, there is no indication that criminals have the intention to use this modus operandi.
Threat Score	1
Vulnerability	This sector requires knowledge and planning expertise which makes it unattractive. Furthermore, given the nature of the business and activity, it is expected to include a low level of cash based and anonymous transactions. The life insurance industry in Gibraltar is a small and long standing sector which has been regulated for many years.
Vuln. Score	1
	2

Risk ID	27
Risk Name	Non-Life Insurance
Description	Perpetrators are using fraud to insurance products to fund their activities (work place insurance, car insurance...)

ML in non-life insurance can occur within the context of, and as the motive behind, insurance fraud, for example where this results in a claim to be made to recover part of the invested illegitimate funds. Relevant risk scenarios are typically focussed on high frequency premiums and cancellations.

Terrorist Financing Risk Assessment

Threat	Gibraltar has not experienced any TF cases within the non-life insurance sector to date. Therefore, there is no indication that criminals have the intention to use this modus operandi.
Threat Score	1
Vulnerability	This sector requires knowledge and planning expertise which makes it unattractive. Furthermore, given the nature of the business and activity, it is expected to include a low level of cash based and anonymous transactions.
Vuln. Score	1
	2

Money Laundering Risk Assessment

Threat	Gibraltar has not experienced any ML cases within the non-life insurance sector to date. Therefore, there is no indication that criminals have the intention to use this modus operandi.
Threat Score	1
Vulnerability	This sector requires knowledge and planning expertise which makes it unattractive. Furthermore, given the nature of the business and activity, it is expected to include a low level of cash based and anonymous transactions.
Vuln. Score	1
	2

Risk ID	35
Risk Name	Couriers in precious metals and stones
Description	Cross-border gold and other precious metal movements – as well as precious stones. Perpetrators who generate cash proceeds seek to convert them into gold and other precious metals or stones and move these profits from their source, either to repatriate funds or to move them to locations where one has easier access to placement in the legal economy. Couriers may use air, sea or rail transport to cross an international border: - containerised or other forms of cargo, concealed in mail or post parcels: If perpetrators wish to move very large amounts of gold and other precious metal, often their only option is to conceal it in cargo that can be containerised or otherwise transported across borders. - sophisticated concealments of gold within goods sent by regular mail or post parcel services.

Terrorist Financing Risk Assessment

Threat	The presence of a Schengen border with Spain where border and customs controls are very strictly enforced mitigates this risk to a very low level.
Threat Score	1
Vulnerability	The presences of a Schengen border with Spain where border and customs controls are very strictly enforced mitigates this risk to a very low level.
Vuln. Score	1
	2

Money Laundering Risk Assessment

Threat	The presence of a Schengen border with Spain where border and customs controls are very strictly enforced mitigates this risk to a very low level.
Threat Score	1
Vulnerability	The presence of a Schengen border with Spain where border and customs controls are very strictly enforced mitigates this risk to a very low level.
Vuln. Score	1
	2

Risk ID	33
Risk Name	High value assets – Precious metals and precious stones
Description	Proceeds of crime (e.g. drug trafficking) are either moved to another country to purchase gold and jewellery which are sold in a third country on the basis of false invoices and certificates, or used directly to buy gold on the national territory and sold to a precious metals broker who then sold it to other businesses. Proceeds of the sale may then be wired to a third party to finance new criminal operations. Criminals favour precious metals and stones which are easy to store and to convert at small costs – which is typically gold and diamonds.

Terrorist Financing Risk Assessment

Threat	There is little trading in precious metals and stones in Gibraltar other than in small retail quantities and of low value/quality.
Threat Score	1
Vulnerability	The OFT are automatically categorising jewellers as high risk businesses. These businesses will all be engaged with to raise awareness and to ensure compliance, including on-site visits.
Vuln. Score	1
	2

Money Laundering Risk Assessment

Threat	There is little trading in precious metals and stones in Gibraltar other than in small retail quantities and mostly of low value. There are only 33 licensed Jewellers trading within Gibraltar, many of which are owned by the same UBO.
Threat Score	1
Vulnerability	The OFT are automatically categorising jewellers as high risk businesses. These businesses will all be engaged with to raise awareness and to ensure compliance, including on-site visits. These businesses have been asked to submit their internal AML/CFT policies and will report annually to the OFT. Specific FATF typologies have been made available on the OFT's website.
Vuln. Score	1
	2

Risk ID	20
Risk Name	Illegal/informal transfer of funds through hawala
Description	Perpetrators are using hawala and informal transfers of funds to channel funds for ML/TF purposes. Perpetrators are attracted since hawala and similar illegal services do not ensure traceability of transactions / reporting of suspicious transactions. The system works via a system of net settlement over a long period of time using banking channels, trade or cash. Contrary to all other remittance systems, funds are not transferred for each and every transaction; Hawala uses net settlement.

Terrorist Financing Risk Assessment

Threat	Those IFT are considered as unregulated payment services under EU law; hence they are illegal within the EU. The size of the problem is not easily identified due to the lack of information.
Threat Score	1
Vulnerability	Those IFT are considered as unregulated payment services under EU law; hence they are illegal within the EU. There is no specific vulnerability assessment for illegal services in the context of the SNRA
Vuln. Score	1
	2

Money Laundering Risk Assessment

Threat	Those IFT are considered as unregulated payment services under EU law; hence they are illegal within the EU. The size of the problem is not easily identified due to the lack of information.
Threat Score	1
Vulnerability	Those IFT are considered as unregulated payment services under EU law; hence they are illegal within the EU. There is no specific vulnerability assessment for illegal services in the context of the SNRA
Vuln. Score	1
	2

Total Risk Score	3
Risk ID	34
Risk Name	High value assets – other than precious metals and stones
Description	Perpetrators use high value goods as an easy way to integrate funds into the legal economy, converting criminal cash into another class of asset which retains its value and may even hold opportunities for capital growth. Certain products such as cars - but also jewellery, watches, luxury boats are particularly attractive as both lifestyle goods and economic assets.

Terrorist Financing Risk Assessment

Threat	Not Relevant
Threat Score	0
Vulnerability	Not Relevant
Vuln. Score	0
	0

Money Laundering Risk Assessment

Threat	Gibraltar has a very limited retail sector area , resulting in limited opportunities for criminals wishing to launder illicit funds through the purchase of High Value Goods. There are only approximately 255 businesses trading within the Main Street Area in total, being the main commercial district and these businesses generally offer moderately high value goods outside Precious metals and stones. This modus operandi is therefore unattractive for criminals criminals wishing to launder illicit funds. Furthermore, most businesses are not inclined to accept large cash transactions due to the high fees imposed by banks when depositing cash. Due to the above the ability for criminals to purchase truly high value items is limited.
Threat Score	2
Vulnerability	Due to the small scale of businesses trading in Gibraltar these HV goods is mitigated considerably as it does not make these entities attractive enough to ML criminals. A lot of the high street shops are geared towards serving one-day tourists looking to purchase duty free items at a lower price than that available in their countries. Tourist are only here for a short period of time and have to pass through a Schengen Border with these goods. Most businesses are not inclined to accept large cash transactions due to the high fees imposed by banks when depositing cash. Due to the above the ability for criminals to purchase truly high value items is limited to easily identifiable businesses in the jurisdiction, which increases the possibility of identification and of a SAR being submitted to the GFIU.
Vuln. Score	1
	3

Total Risk Score	2
Risk ID	51
Risk Name	Identity Theft
Description	That launderers or terrorist financiers acquire false identity documentation in order to obtain services and products.
Terrorist Financing Risk Assessment	
Threat	Not considered at present a TF risk
Threat Score	0
Vulnerability	Not considered at present a TF risk
Vuln. Score	0
	0
Money Laundering Risk Assessment	
Threat	The separation of the benefits of criminal or terrorist activity from the physical person who has committed the act has always been one of the main focuses of criminals so that they can derive the benefit of the criminal activity with anonymity. If a criminal can obtain financial or other products in a false name then they can continue to use the same without a direct link to their person.
Threat Score	1
Vulnerability	The increase in utility and other bills which are delivered electronically, that can easily be doctored or forged, makes their value in verifying addresses as part of a due diligence process considerably diminished. Gibraltar's finance industry CDD procedures are well developed allowing the better detection of false identity documents. However the pre-paid credit card and gaming industry which often conducts remote CCD may be more susceptible to the use of false identification. The remote nature of the customer base may provide the customer with greater opportunities to use false identifications without the physical checking of identification documents and their authenticity. False documentation usually comes in two forms, either stolen identities using real documents or false identities using false documents. There are experiences of both in Gibraltar.
Vuln. Score	1
	2

