



National Coordinator for AML/CFT

2025 National Risk Assessment

Money Laundering, Terrorist Financing, Proliferation
Financing, Illegal Wildlife Trade, Human Trafficking,
Sanction Circumventions Risk and Tax Crime Risk.

August 2025

V1.2



1	MINISTERIAL FOREWORD.....	4
2	INTRODUCTION.....	5
2.1	Previous National Risk Assessment Processes.....	5
2.2	EU Supra National Risk Assessment	5
2.3	Use of the NRA by competent authorities.....	5
2.4	Use of the NRA by the private sector	5
2.5	Contact.....	6
3	RISK AND CONTEXT	6
4	METHODOLOGY AND CONSTRUCTION OF THE NRA.....	7
4.1	Threat and Vulnerability Assessment	8
5	GEOGRAPHIC RISK.....	9
5.1	Spain	9
5.2	Morocco	10
5.3	United Kingdom.....	11
5.4	Sanction Circumvention Risk	12
5.5	High risk jurisdictions	12
5.6	EU and EEA Jurisdictions	17
6	TRANSNATIONAL CRIMES	17
6.1	Mutual Legal Assistance	17
6.2	Organised Crime Groups	20
6.3	Tobacco	21
6.4	Drug Trafficking	22
6.5	Fraud.....	23
6.6	Cyber enabled Fraud	23
6.7	Money Laundering / Proceeds of Crime.....	24
6.8	Bribery & Corruption.....	24
6.9	Cash & Cash couriers.....	24
6.10	Trade Based Money Laundering	29
6.11	Modern Slavery, Human Trafficking and Migrant Smuggling (MSHT)	29
6.12	Illegal Wildlife Trade.....	31
7	SECTORAL ASSESSMENTS.....	32
7.1	Banking	32
7.2	Trust and Corporate Services Providers	39
7.3	Money Services Businesses (MSBs) and Money Value Transfer Services (MVTs).....	62
7.4	Securities Sector.....	66
7.5	Funds Sector	68
7.6	E-Money	77
7.7	Virtual Asset Service Providers (VASPs)	81
7.8	Gambling.....	89
7.9	Insurance Sector	95
7.10	Real Estate	98
7.11	High Value Dealers	101
7.12	Legal Professionals	103
7.13	Composition and materiality.....	103
7.14	Types of Relevant Financial Business.....	104
7.15	RFB transaction clients	106
7.16	Auditors and Insolvency Practitioners	109
7.17	Accountants.....	111
7.18	Tax Advisors	113



7.19	Pensions Advisors and Pension Scheme Operators	115
7.20	Domestic Football League.....	117
8	JURISDICTIONAL TERRORIST FINANCING RISK	118
8.1	Extreme Right-Wing Terrorism	119
8.2	Likelihood of a terrorist attack in Gibraltar.....	119
8.3	Hawala.....	119
8.4	Abuse of Non-Profit Organisations	120
9	SANCTION CIRCUMVENTION RISK.....	121
9.1	Gibraltar's Obligations to Comply with Sanctions Regimes	121
9.2	The Role of Regulated Entities in Preventing Sanctions Circumvention ..	121
9.3	Compliance and Enforcement Mechanisms.....	128
9.4	Conclusion.....	128
10	PROLIFERATION FINANCING.....	128
11	TAX CRIME RISK.....	138
11.1	Introduction	138
11.2	Domestic framework.....	139
11.3	International tax cooperation, transparency and exchange of information.....	140
11.4	Strategic Approach.....	144
11.5	Conclusion.....	146
12	SUMMARY OF RISKS, THREAT AND VULNERABILITY SCORES	146



1 Ministerial Foreword

It is my pleasure to present the latest National Risk Assessment (NRA) on Gibraltar's risk landscape. This document is an important milestone in our ongoing commitment to meet the highest international standards under the FATF framework.

Since Gibraltar's removal from the FATF Grey List in February 2024, we have worked tirelessly to consolidate progress and strengthen our compliance further. Over the past year, we have enhanced our financial crime framework through new measures such as Unexplained Wealth Orders, improved information sharing, and greater law enforcement capability. We have prioritised key areas including risk-based supervision and beneficial ownership transparency.

Our efforts have been recognised internationally. The European Commission's recent removal of Gibraltar from the EU list of high-risk jurisdictions reflects both our technical compliance and our determination to safeguard the integrity of our financial system.

But we must not stand still and must redouble our efforts where necessary.

Looking ahead, we are preparing for Gibraltar's next Moneyval evaluation in 2027 under the revised FATF Standards, which sets an even higher bar for both technical and effectiveness compliance. This NRA provides an understanding of our risk landscape and will guide our response over the coming years.

Further, the EU political agreement on Schengen marks a significant and positive step forward for Gibraltar. Its implementation will have to be monitored closely for its impact on this NRA and our preparations for the forthcoming evaluation.

I wish to thank all our stakeholder authorities and private sector partners for their dedication to protecting Gibraltar's reputation and ensuring the resilience of our financial system. Together, we must continue to demonstrate that Gibraltar is a trusted, responsible, and proactive jurisdiction in the global fight against financial crime.

Our objective is clear: to prevent illicit funds from entering our economy or financial system, and safeguarding Gibraltar's position as a secure, reputable, and attractive place to do business.

The Hon. Mr Nigel Feetham KC MP
Minister for Justice, Trade and Industry
HM Government of Gibraltar

August 2025

2 Introduction

This National Risk Assessment (NRA) is the latest iteration of the process by Gibraltar that seeks to identify threats and vulnerabilities in Money Laundering (ML), Terrorist Financing (TF) as well as Proliferation Financing (PF), Sanction Circumvention and Tax Crime Risk, amongst others, as it affects Gibraltar as a jurisdiction as well as public sector bodies and the private sector.

The purpose of the NRA is to provide a realistic strengths-weaknesses analysis in the field of ML and TF in Gibraltar and to identify existing and future risks and map them effectively.

2.1 Previous National Risk Assessment Processes

This NRA is the fourth iteration of a National Risk Assessment (NRA) for Gibraltar with previous versions having been published in 2016, 2018 and 2020. Since 2020, the NRA process has also included a jurisdictional TF assessment, as well as higher risk sectors.

This version of the NRA builds on the knowledge gained from the experience of the previous NRA documents and feedback from the private as well as public sector.

2.2 EU Supra National Risk Assessment

Under the National Coordinator for Anti-Money Laundering and Combatting Terrorist Financing Regulations 2016, the National Co-Ordinator (NCO) must consider the findings of the EU's Supra National Risk (EUSNRA) Assessment in its own considerations. The EUSNRA was recently updated, and it is therefore essential that those findings have already found their way into Gibraltar's NRA processes.

2.3 Use of the NRA by competent authorities

In reviewing the findings of the NRA, competent authorities (public sector authorities, law enforcement agencies, Gibraltar Financial Intelligence Unit and regulators) need to design action plans that seek to lower the overall risk that each of the threats present both to ML and TF, and where applicable, also PF.

Mitigation programmes may need to address risks separately as the threats and vulnerabilities presented by each risk may have a different profile and one approach may not cover both.

The mitigation programme by the public sector will be supported by a National Strategy which seeks to mitigate the risks through targeted actions.

2.4 Use of the NRA by the private sector

Under the Proceeds of Crime Act (POCA), Relevant Financial Businesses (RFBs) are required to consider the NRA in their own risk assessment frameworks to ensure that their systems of controls are commensurate with the risks present in Gibraltar.

POCA does not permit a RFB to arrive at a conclusion on risk which is incompatible with the findings of this NRA and therefore any application of simplified or enhanced Customer Due Diligence (CDD) must be made in light of the NRA findings.

By providing the private sector with clear indicators of those products, services and sectors which could potentially prove attractive to either ML or TF in the NRA this should aid compliance officers and risk managers in making suspicious activity reports (SARs) of a

higher quality and focus their attention to those products and services of their firms which the NRA identifies as a higher risk.

2.5 Contact

This publication is available at:

<https://www.gibraltar.gov.gi/finance-gaming-and-regulations/financial-crime>

Any enquiries regarding this publication should be sent to:

Annette Perales

Ministry for Justice, Trade and Industry

HM Government of Gibraltar

nco@gibraltar.gov.gi

3 Risk and Context

Gibraltar is a small finance centre which is largely UK customer centric in financial services and on-line gambling. Traditional financial services products for Gibraltar had been the provision and servicing of corporate structures and private banking. Over the last two decades these services have been in decline and replaced with on-line gambling, e-money products and more recently, Distributed Ledger Technologies/ Virtual Assets Service Providers (DLT/VASP).

The changing landscape of products and services necessitates that we carefully consider new and emerging risks and implement mitigation programmes to effectively mitigate the threats and vulnerabilities present in the jurisdiction.

Gibraltar's client base is largely non-resident and sourced in a non face-to-face way. Both factors increase the inherent risk.

As a finance centre the products and services available to customers and potential customers may be accessed from anywhere in the world and many may be used in jurisdictions worldwide. With the threat of use of funds to fund either terrorist organisations, terrorists or supporting terrorist activities in general, the public and private sector need to remain vigilant to the use of their products and service in countries or areas close to conflict zones or those where there is a linkage to terrorist activities.

Since Gibraltar's removal from the FATF grey list, the Government has significantly strengthened the capability of law enforcement agencies by increasing resources and delivering specialist training to enhance the investigation of complex financial crime. Given Gibraltar's small size, the most complex drug-related and money laundering cases involve cross-border elements and sophisticated methodologies, necessitating close cooperation with overseas counterparts. The jurisdiction's priority is to ensure enhanced inter-agency coordination, that cases of suspicious activity are thoroughly investigated and pursued by local agencies and that the evidence is capable of supporting successful prosecutions where offences are identified.

It is important to note Gibraltar's current and evolving political landscape when assessing existing and emerging risks. In particular, attention is drawn to the announcement made in

June 2025 regarding a political agreement between the United Kingdom and the European Union for the conclusion of a treaty concerning Gibraltar's future relationship with the EU, including with the Schengen area.

The conclusion and implementation of a treaty will result in legal, regulatory, and operational changes. These would primarily affect areas such as border controls, data sharing, law enforcement cooperation, and the movement of persons. In turn, these changes may have consequential impacts on Gibraltar's exposure to money laundering (ML) and terrorist financing (TF) risks, as well as on supervisory frameworks and Gibraltar's broader international obligations.

This NRA has been developed based on the prevailing legal and institutional framework at the time of publication. However, stakeholders should remain mindful that Gibraltar's risk landscape and legal context may be subject to material changes in the short to medium term. As such, future iterations of the NRA will need to fully incorporate and reflect these developments.

In the interim, competent authorities, regulated entities, and other relevant stakeholders are encouraged to monitor ongoing political and legal developments. Proactive consideration should also be given to the potential strategic and operational implications of Gibraltar's expected alignment with key aspects of the Schengen acquis.

4 Methodology and Construction of the NRA

The NRA builds on the previous NRAs and the updated EUSNRA. These have been supplemented by additional and more comprehensive data sets that are available from the public sector which provides a granular level of detail of transaction data in the financial services sector as well as data from law enforcement agencies (LEAs), Gibraltar Financial Intelligence Unit (GFIU) as well as incoming and outgoing international co-operation data including Mutual Legal Assistance (MLA).

In arriving at the overall risk score for each of the sectors, products and services the threat and vulnerability to ML and TF risks have been assessed separately. The combined score is a useful indicator but does not replace the need for users of this NRA to consider the risks separately as it may affect their own circumstances.

The development of the NRA is led by the National Coordinator for AML/CFT taking into account as many inputs as possible and importantly the support from competent authorities who have led in the identification and refinement of the threat assessments with their knowledge and expertise. Similarly, private sector input is invaluable as the 'coal face' in the fight against ML/TF through the intimate understanding of their own product vulnerabilities. For this reason, both public and private sector bodies have been invited to provide direct input into the NRA so as to better calibrate the final NRA output.

Competent Authorities	Private Sector Bodies
Gambling Commissioner	Association of Trust and Company Managers Ltd
Gibraltar Centre for Criminal Intelligence Department	Gibraltar Betting and Gaming Association
Gibraltar Financial Intelligence Unit	Gibraltar Association for New Technologies

HM Customs Gibraltar	Gibraltar Association of Compliance Officers
Legal Services Regulatory Authority	Gibraltar Association of Pension Fund Administrators
Office of Criminal Prosecutions & Litigation	Gibraltar Association of Pensions Fund Administrators
Office of Fair Trading	Gibraltar Federation of Small Businesses
Income Tax Office	Gibraltar Banker's Association
Royal Gibraltar Police	Gibraltar Chamber of Commerce
Gibraltar Financial Services Commission	Gibraltar E-Money Association
	Gibraltar Funds and Investments Association
	Gibraltar Insurance Association
	Gibraltar Society of Accountants
	Law Council
	Society of Trust and Estate Practitioners

TABLE 1 - LIST OF TRADE ASSOCIATIONS AND AUTHORITIES CONSULTED IN THIS NRA PROCESS

The involvement of public and private sector bodies in the NRA process makes the outcomes more credible and useful for all parties.

4.1 Threat and Vulnerability Assessment

Threat refers to an activity that has some potential for damage (or could cause harm) in connection with relevant forms of crime or the financing of terrorist activities. Vulnerability, on the other hand, means gaps or ambiguities in the existing defence mechanism to prevent and combat money laundering and Terrorist financing in Gibraltar. A threat- as well as a potential vulnerability can be made at both national and sector level, which is why, in the context of this NRA, the threat situation and the vulnerability at both national and sectoral level in terms of money laundering and terrorist financing have been analysed.

Scoring for threat and vulnerability is on the following basis individually for ML and TF risks;

Score	Description
0	Not Applicable
1	Lowly Significant
2	Moderately Significant
3	Significant
4	Very Significant

TABLE 2 - THREAT AND VULNERABILITY SCORING

The combined threat and vulnerability score for each ML and TF provide the **ML or TF risk score** for that risk on a scale of;

Score	Description
0	Not Applicable

2 to 3	Low Risk
4 to 6	Medium Risk
7 to 8	High Risk

TABLE 3 - RISK SCORING

5 Geographic Risk

5.1 Spain

As our closest neighbour with whom daily trade is conducted across all sectors of the economy, Gibraltar needs to be aware of the ML and TF risks present in that country and how these could affect Gibraltar.

Spain's most recent FATF follow-up report is to be found at <https://www.fatf-gafi.org/media/fatf/documents/reports/fur/Follow-Up-Assessment-Spain-2019.pdf> and it is interesting to note the inclusion of Organised Crime in the Campo area as the top ML risk for Spain. The report states;

"11. Spain continues to be exposed to organised crime due to its geostrategic position as a point of access to the European Union. As a consequence, the main ML threats are related to the activities of Organised Criminal Groups (OCGs) based in North Africa, Latin America and the former Soviet Union involved in drug crimes, organised crime, tax and customs offences, as well as counterfeiting and human trafficking. Risks emanating from the OCGs operating in the Campo de Gibraltar area have become of increased focus by authorities.

...

14. Spain continues to face a high risk of TF from Islamic terrorist groups, including a slight increase in the risks of returning foreign terrorist fighters. Risk of radicalised individuals, supporting terrorist organisations by providing funds, including through the misuse of MVTs providers, remains to be among the key challenges for the competent authorities of Spain. Some types of NPOs continue to be vulnerable to TF abuse as well."

A lot of positive steps have been taken by the Spanish State and its law enforcement agencies to reduce the impact of OCG activities, particularly in the Campo de Gibraltar, over recent years.

However, the *Informe Anual de Seguridad Nacional 2023* of the Spanish Government¹ provides a detailed account of the challenges posed by organised crime groups in the regions of Algeciras and the Costa del Sol. These areas have become focal points for drug trafficking, with the ports serving as major entry points for narcotics such as cocaine from Latin America and hashish from North Africa. These activities are facilitated by well-organised criminal networks that have established strong footholds in these regions.

The report highlights the increasing violence and turf wars among rival gangs in the Costa del Sol, where the competition for control over lucrative trafficking routes has led to a surge in violent incidents, including murders and kidnappings. This intense rivalry reflects the high stakes involved in controlling these routes, which are vital for the transportation of drugs into Europe.

¹ <https://www.dsn.gob.es/es/documento/informe-anual-seguridad-nacional-2023>

In response to these challenges, Spanish authorities have stepped up their efforts to combat organised crime. The report commends the significant seizures of drugs and the arrests of key gang members, resulting from intensified law enforcement operations. These efforts have been bolstered by strong collaboration between national and international law enforcement agencies, which has been crucial in disrupting the operations of these criminal groups.

Furthermore, the report addresses the pervasive issue of money laundering associated with organised crime in these regions. Criminal organisations use various methods, including real estate investments and luxury goods purchases, to launder the proceeds of their illicit activities. This not only sustains their operations but also integrates criminal proceeds into the legitimate economy, complicating efforts to trace and confiscate illegal gains.

Organised crime continues to affect local communities in Algeciras and along the Costa del Sol. The report highlights the importance of maintaining and strengthening strategies aimed at supporting community safety and resilience in the face of these challenges.

Overall, the *Informe Anual de Seguridad Nacional 2023* paints a comprehensive picture of the ongoing battle against organised crime in Spain's strategic regions of Algeciras and the Costa del Sol, highlighting the complex interplay of drug trafficking, violence, and money laundering, as well as the concerted efforts of law enforcement to mitigate these threats.

Spain will therefore remain as presenting a high risk of ML.

Risk mitigation measures put in place by individual regulated entities may permit each regulated entity to reduce the country risk of Spain to a lower level but the reasons and methodology how the regulated entity has arrived at this lower score must be documented and demonstrable. At no time, however, can a regulated entity consider that the country risk is Low Risk nor that any customer with a connection (residency, nationality or economic activity) to Spain can be subject to Simplified Due Diligence.

TF Assessment

Gibraltar needs to be aware of the TF risks present in Spain given she is our closest neighbour with whom daily trade is conducted across all sectors of the economy. There have been a number of counter terror arrests in the first half of 2024 in Spain including two involving TF related activities linked to crypto currencies.

Spain's FATF follow-up report notes that:

"Spain continues to face a high risk of TF from Jihadist terrorist groups, including a slight increase in the risks of returning foreign terrorist fighters.

The risk of radicalised individuals supporting terrorist organisations by providing funds, including through the misuse of MVTs providers, remains to be among the key challenges for the competent authorities of Spain.

Some types of NPOs continue to be vulnerable to TF abuse as well."

The TF risk posed to Gibraltar by **Spain has been assessed in the NRA as being high.**

5.2 Morocco

In much the same way that physical proximity is a factor with Spain, Morocco needs to be accounted for in terms of a jurisdictional risk assessment. Morocco is known for its production of cannabis, with some of the product trafficked through the Strait of Gibraltar (although not through Gibraltar or British Gibraltar Territorial Waters (BGTW)).

Additionally, there are concerns about potential terrorist financing risks linked to migration from certain parts of northern Africa and the Sahel. However, Morocco's efforts to be removed from the FATF Grey List reflect progress in addressing their ML vulnerabilities.

ML & TF Assessment

Morocco is one of the leading cannabis producers in the world, supplying most of Europe's demand for the product. Although Gibraltar sits between long-established trafficking routes for drugs and migrant smuggling, it is not a destination point.

The increase in radicalisation in Northern Africa and the Sahel has led to a corresponding rise in the threat of terrorist activity, and therefore an increased TF risk arising from migration from these regions.

In addition to the involvement of organised criminal groups (OCGs) in drug trafficking, Moroccan OCGs also have a significant presence in migrant smuggling into the EU.

Morocco's mutual evaluation report was published in April 2019 and notes that:

"Terrorism and its financing still pose a serious threat to Morocco despite the significant efforts exerted by competent authorities in combating terrorism; this threat mainly stems from Moroccan FTFs whose number is estimated to be around 1600. In addition to the risks resulting from terrorist organizations, such as Daesh and threats related to Al-Qaida, mainly its branch known as "Al-Qaida in the Islamic Maghreb", despite their declining activity following the emergence of the terrorist organization Daesh, as well as the threats posed by the terrorist group "Islamic Movement of the Levant".

There are no known links between OCGs operating in the Campo de Gibraltar area and Terrorist Organisations (TOs). However, given TOs tend to engage in or be funded by criminal activities, the possibility that the North African element of the OCG operations is supporting TOs cannot be excluded.

The ML & TF risk posed to Gibraltar by **Morocco has been assessed in the NRA as being High.**

Risk mitigation measures put in place by individual regulated entities may permit each regulated entity to reduce the country risk of Morocco to a lower level but the reasons and methodology how the regulated entity has arrived at this lower score must be documented and demonstrable. At no time, however, can a regulated entity consider that the country risk is Low Risk.

5.3 United Kingdom

As the main trading partner for Gibraltar in terms of its financial and gaming services and products it is natural to include an assessment of the UK as part of a comprehensive NRA process.

The ties between Gibraltar and the UK are historically strong, resulting in a significantly higher volume of cross-border activity compared to other jurisdictions. Gibraltar's legal and regulatory framework, especially in relation to company and trust structures, closely aligns to that of the UK. While this alignment offers practical and legal familiarity, it may also facilitate certain types of financial transactions across borders.

This similarity is not inherently problematic; however, it can create an environment where UK-based individuals involved in money laundering (ML) may perceive Gibraltar as a more accessible or comfortable jurisdiction. The shared structures and regulatory approaches may be viewed as more accommodating than those in other jurisdictions with unfamiliar regimes.

ML & TF Assessment

Whilst the United Kingdom may be some distance away, Gibraltar's close political and economic links with it warrants giving it individual consideration. Their most recent mutual evaluation report notes:

"The UK faces severe threats from international terrorism. Terrorist financing activity in the UK is usually low-level, involving small amounts of funds raised by UK based individuals to fund their own travel to join terrorist groups, to send to terrorist associates, or to finance their own terrorist attack plans. The UK also faces threats from Northern Ireland-related terrorism which are rated severe in Northern Ireland and substantial in Great Britain. The nature of the Northern Ireland-related terrorism threat has evolved with paramilitaries and terrorist groups focusing on forms of organised crime which are not all specifically intended to raise funds for terrorism."

The ML & TF risk posed by **the UK has been assessed as Medium and Low respectively.**

Risk mitigation measures put in place by individual regulated entities may permit each regulated entity to reduce the country risk of the UK to a lower level but the reasons and methodology how the regulated entity has arrived at this lower score must be documented and demonstrable.

5.4 Sanction Circumvention Risk

Please see new Chapter 8 dealing exclusively with the risk of sanction circumvention and how countries that are subject to UK, European Union or United Nations Sanctions regimes are to be treated.

5.5 High risk jurisdictions

Gibraltar, as a regional financial centre conducts transactions not only with the UK but many other jurisdictions throughout the world. Businesses must be aware that each country presents different risks to both money laundering and terrorist financing either because of the prevalence of certain predicate offences, the funding of terrorist activities or the lack of effective controls to prevent either. Fortunately international standard setting bodies like the FATF and its regional bodies conduct detailed evaluations of the effectiveness of controls in each jurisdiction and these reports can easily be accessed from [http://www.fatf-gafi.org/publications/mutualevaluations/?hf=10&b=0&s=desc\(fatf_releasedate\)](http://www.fatf-gafi.org/publications/mutualevaluations/?hf=10&b=0&s=desc(fatf_releasedate)).

In more general terms the Gibraltar Financial Services Commission (GFSC), as the primary financial services regulatory authority, uses a much broader definition of High-Risk Jurisdictions than the narrower FATF definition as it captures in its regulatory returns transaction data with countries that are either drug producers or transit countries for drugs and conflict zones and countries close to those. This, however, does not mitigate the need for vigilance either for the transaction themselves or from customers and business relationships with these countries.

FATF High Risk Jurisdictions

The FATF maintains a list of monitored countries <http://www.fatf-gafi.org/countries/#high-risk> which are;

Jurisdictions under Increased Monitoring as of June 2025:

Algeria, Angola, Bolivia, British Virgin Islands, Bulgaria, Burkina Faso, Cameroon, Côte d'Ivoire, Democratic Republic of the Congo, Haiti, Kenya, Lao People's Democratic

Republic, Lebanon, Monaco, Mozambique, Namibia, Nepal, Nigeria, South Africa, South Sudan, Syria, Venezuela, Vietnam, and Yemen.

Regulated entities should ensure that they continuously monitor the FATF Grey and Black lists as territories are being added and removed at least twice a year. It should also be noted that there is no need to de-risk from a country merely because it appears on the FATF grey list but regulated entities should, on the basis of their risk based approach make their own determination as to what additional mitigation measures might be necessary when dealing with these countries.

Gibraltar's customer base in financial services is only marginally derived from FATF high risk jurisdictions.

Transactions and business relationships with these countries are susceptible, because of the lack of effective measures to prevent ML and/or TF, to both types of risks.

Conflict Zones

The GFSC has considered the following criteria in the analysis of which countries fall into this category;

- A conflict zone. This is a synonymous term for those high-risk jurisdictions/regions that are unstable, at war, where armed hostility is present or where terrorist organizations are active.
- Provinces/regions with known links to terrorist organizations or share a border with territories controlled by terrorist organizations.
- Countries where funds and other assets are generated (e.g., originator of the funds transfer) for terrorism acts or terrorist organizations irrespective of where those acts take place or organizations reside.
- Jurisdictions/regions that are transit points or have had money flows to/from known foreign-terrorist fighters (FTFs).

In doing so the following countries have been considered as falling into this category;

Afghanistan, Belarus, Burkina Faso, Burundi, Cameroon, Central African Republic, Chad, China, Congo, Democratic People's Republic of the Congo, Republic of the Congo, Egypt, Ethiopia, Gambia, Guinea, Haiti, Iran, Islamic Republic of Iraq, Israel, Democratic People's Republic of Korea (North), Lebanon, Libya, Mali, Mauritania, Mexico, Myanmar, Niger, Nigeria, Pakistan, Palestine, Russia, State of, Sahel, Senegal, Somalia, South Sudan, Sudan, Syria (Syrian Arab Republic), Türkiye, Uganda, Ukraine, Venezuela, Yemen.

Transactions and business relationships with conflict zones may be susceptible to TF risks. There have been numerous cases of TF facilitators located in jurisdictions neighbouring a conflict to assist in transporting funds and other goods (including foreign terrorist fighters) into or out of conflict zones. Although Gibraltar is not itself close to a conflict zone the assessment conducted by the GFSC on the inflows and outflows of funds by the financial services industry has identified a small number of transactions received from and issued to such jurisdictions. E-money products were the most widely used products in these conflict zone jurisdictions, however, the average value of the transactions is low. Banking transactions with these jurisdictions, whilst fewer in number, are generally of a higher value. This is to be expected given that the banking system is generally used to transfer larger amounts of money than e-money, in which the sums tend to be very low and related to individual or personal expenses. Operators must be extremely cautious when transacting with entities that are based in or linked to these countries.



Data 2023 and 2024

The following table shows the value and number of transactions for all financial services sectors for the years 2023 and 2024 with Conflict Zones and drug producing or transit jurisdictions:

		No. Transactions Received		No. Transactions Issued		Value of Funds Received (£)		Value of Funds Issued (£)	
		2023	2024	2023	2024	2023	2024	2023	2024
Conflict zone & produces &/or transits drugs	Afghanistan, Islamic State of	0	0	12	0	£0	£0	£1,331	£0
	Haiti	9	3	0	1	£38,899	£9,067	£0	£180
	Mexico	213	312	16163	25845	£500,943,509	£6,033,627	£2,832,507	£3,158,097
	Myanmar	0	0	0	3	£0	£0	£0	£19
	Pakistan	134	42	3731	10992	£11,949	£53,788	£530,468	£526,322
Conflict Zones	Venezuela, Bolivarian Republic of	0	1	9	630	£417	£0	£1,394	£5,894
	Belarus	1	13	28	8	£0	£9,843	£7,423	£6,450
	Burkina Faso	0	0	31	5	£0	£0	£284	£1,113
	Burundi	0	0	0	227	£0	£0	£0	£2,860
	Cameroon	3	10	93	1	£302	£212,061	£10,747	£186,966
	China, People's Republic of	601	968	4535	17594	£969,432	£3,655,791	£11,906,703	£8,910,160
	Congo, Democratic Republic of the	3	7	45	55	£259,712	£1,716,141	£392,686	£29,235
	Congo, Republic of the	0	0	122	43	£0	£0	£451,279	£120,090
	Egypt	101	144	7588	17285	£535,192	£428,011	£3,311,713	£2,383,837
	Ethiopia	3	0	980	752	£1,117	£0	£94,099	£112,681



	Gambia	5	5	131	171	£123,130	£16,860	£8,193	£12,561
	Guinea	0	0	1	21	£0	£0	£9,222	£5,852
	Iraq	1	0	5	29	£58	£0	£212	£4,147
	Israel	371969	292588	243,402	203306	£47,618,452	£58,343,624	£274,430,101	£303,648,218
	Korea, Democratic People's Republic of (North)	0	0	0	0	£0	£0	£0	£0
	Lebanon	2	3	90	148	£1,058	£2,879	£43,177	£31,650
	Mali	2	7	0	0	£692,756	£7,940,526	£0	£0
	Mauritania	0	0	2	1	£0	£0	£179	£255,344
	Niger	0	1	1	7	£0	£757	£1	£607
	Nigeria	92	82	3443	7052	£196,335	£807,978	£2,480,141	£1,891,254
	Palestine, State of	1	0	791	857	£68	£0	£174,172	£145,136
	Russian Federation	9	0	9	1	£1,793,159	£0	£450,659	£684
	Senegal	1	0	382	287	£399	£0	£255,984	£32,052
	Somalia	0	0	6	1	£0	£0	£505	£254
	Türkiye	1929	1054	81790	141326	£5,894,561	£13,478,815	£9,315,472	£14,773,365
	Uganda	14	16	627	596	£18,918,610	£24,917,846	£3,065,884	£186,869
	Ukraine	1	251	1731	4644	£7,887	£31,970	£1,569,952	£1,922,111
	Yemen	2	1	14	0	£75,756	£8,286	£1,666	£0
Produces &/or transits drugs									
	Bahamas	40419	188	1475	2291	£7,892,611	£13,046,092	£9,029,412	£4,059,341
	Belize	24	7	319	741	£303,975	£153,774	£59,682	£51,975
	Bolivia	7	22	285	387	£30,933	£189,073	£48,884	£21,416
	Colombia	104	241	6817	11693	£6,145,263	£6,509,098	£1,447,294	£4,861,522
	Costa Rica	20	23	2434	4029	£257,779	£37,637	£2,086,134	£943,934
	Dominican Republic	22	19	3065	5641	£413,638	£217,437	£366,827	£494,560
	Ecuador	8	11	873	1179	£129,643	£159,674	£760,555	£390,714
	El Salvador	11	13	106	539	£322,485	£165,958	£47,743	£390,714



Guatemala	5	12	256	884	£2,866	£87,117	£350,305	£56,401
Honduras	2	7	963	1929	£46,891	£47,607	£54,587	£319,488
India	744	1201	19754	35306	£9,287,827	£4,290,681	£131,776,249	£169,000,800
Jamaica	29	26	4101	7488	£14,174	£13,666	£223,596	£610,522
Lao People's Democratic Republic	0	0	5	0	£0	£0	£35,616	£0
Nicaragua	6	12	192	953	£74,121	£99,206	£21,935	£85,470
Panama	30	122	3402	6846	£1,219,706	£2,149,175	£3,155,902	£6,809,567
Peru	26	121	3091	6846	£366,847	£2,589,931	£16,619,262	£5,792,343
Total	416553	297533	412900	518640	£604,593,540	£147,423,996	£477,430,137	£532,242,775

TABLE 4 - HIGH RISK JURISDICTION TRANSACTION DATA FOR 2023 AND 2024



5.6 EU and EEA Jurisdictions

A general assumption made in determining geographic risk is that because a country is required to transpose EU Anti Money Laundering Directives as well as other financial services Directives relating to the freedom of movement of capital (e.g. passporting rights) that all EU and EEA states will have broadly similar, lower risk of ML and/or TF.

As the FATF Mutual Evaluation processes clearly demonstrate such an assumption cannot be automatically reached and business should make their own assessment, based on the published results as to whether an EU/EEA State meets the required standards.

6 Transnational Crimes

6.1 Mutual Legal Assistance

Mutual Legal Assistance (MLA) is the formal method of co-operation between countries for obtaining assistance in the investigation and prosecution of criminal offences so that the evidence gathered can be used in legal proceedings. Gibraltar can provide a wide form of assistance, including assistance in non-conviction based investigations and proceedings.

The MLA Department which sits within the Office of Criminal Prosecutions & Litigation is the Competent Authority for receiving and processing MLA requests on behalf of the Attorney General. The Central Authority is the Minister for Justice.

Between 2019 and 2024, Gibraltar received a total of 322 MLA requests from 45 different countries. During this period, the most requests were received from the United Kingdom (76), Spain (44) and Germany (35) followed by the Netherlands and Poland (18 each), Switzerland and Portugal (10 each) and other jurisdictions sending less than 10 each.

YEAR	2019	2020	2021	2022	2023	2024
No. of MLA Requests received	88	56	47	49	35	47

TABLE 5 - NO. OF MLA REQUESTS RECEIVED

Data obtained through MLA is considered and assists in assessing Gibraltar's threats and vulnerabilities. The predicate offences for which MLA is sought provides a good indicator of Gibraltar's ML and TF risks.

Offences	2019	2020	2021	2022	2023	2024	TOTAL
Betting without a licence	0	2	0	1	1	0	4
Blackmail	0	2	0	0	0	0	2
Bribery & Corruption	1	1	0	2	0	4	8
Child pornography	0	1	0	0	0	0	1
Computer fraud	10	8	4	1	2	0	25
Computer misuse	0	0	0	0	1	2	3
Contempt of Court	0	1	1	0	0	0	2
Driving offence	1	1	1	0	0	1	4
Drug trafficking	11	5	4	7	4	5	36
Embezzlement	0	0	2	1	0	2	5



Offences	2019	2020	2021	2022	2023	2024	TOTAL
Forgery	0	1	2	1	1	2	7
Fraud	33	18	15	13	13	14	106
GBH	0	0	1	0	0	0	1
Human Trafficking	3	0	0	0	0	0	3
Match fixing	0	0	0	0	1	0	1
Money Laundering only	12	6	7	5	3	2	35
Money Laundering	6	4	1	2	4	0	17
Murder	0	1	2	0	1	3	7
Rape	1	2	0	1	0	2	6
Robbery/Theft	4	0	2	5	0	0	11
Breach of Sanctions	2	0	0	0	0	1	3
Sexual assault	0	0	0	5	1	1	7
Tax	2	3	5	4	2	4	20
Torture	0	0	0	1	0	0	1
Trademark infringement	1	0	0	0	0	0	1
Unknown	0	0	0	0	1	0	1
Firearms	0	0	0	0	0	1	1
Companies Act offence	0	0	0	0	0	2	2
Possession of an offensive weapon	0	0	0	0	0	1	1
TOTAL	87	56	47	49	35	47	321

TABLE 6 - PREDICATE OFFENCE INDICATED IN MLA REQUESTS

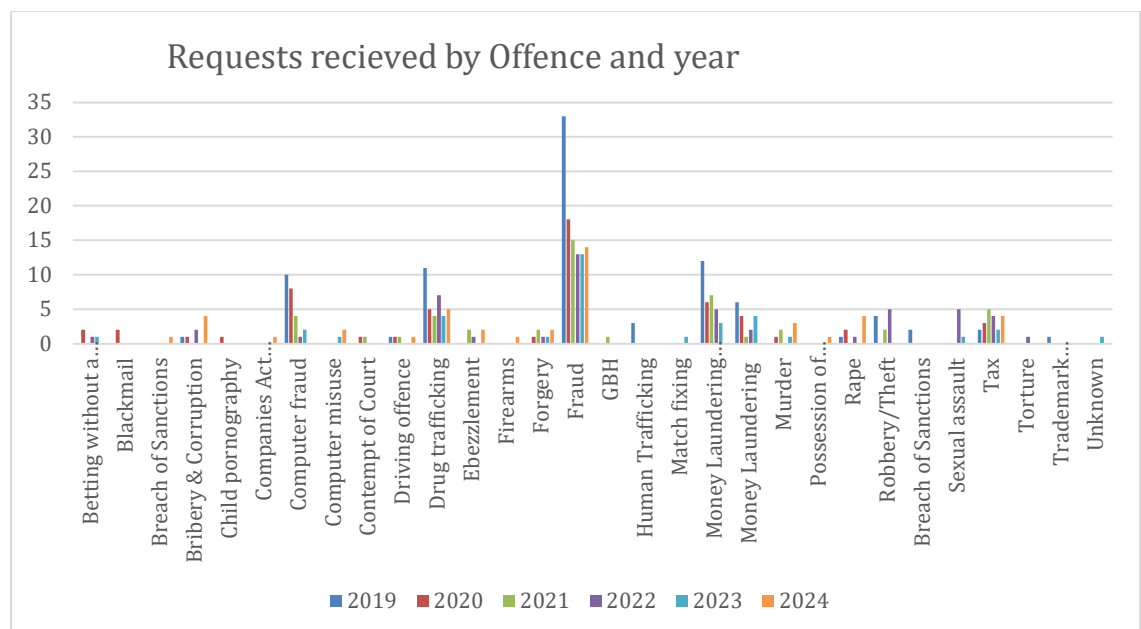


FIGURE 1 - REQUESTS RECEIVED BY OFFENCE AND YEAR

The highest number of MLA requests relate to fraud (131), when combining fraud and computer fraud, which represents 41% of requests received. This is followed by money laundering (52), combining 35 in connection with requests involving money laundering only and those where it predominately relates to money laundering (17), which represents 16% of requests received. The third most common predicate offence is drug trafficking (36) which represents 11% of requests received.

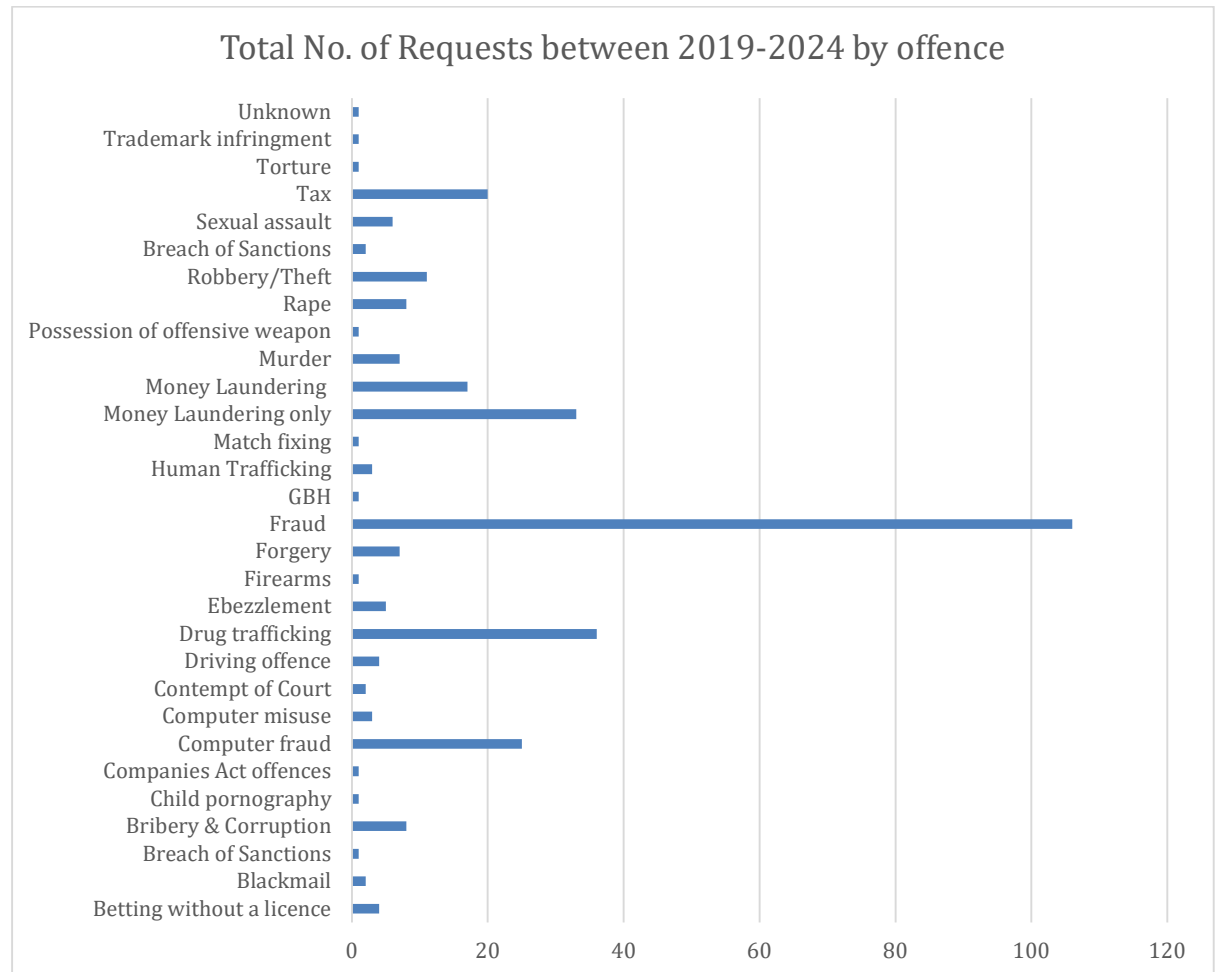


FIGURE 2 - TOTAL NO. OF REQUESTS RECEIVED BETWEEN 2019-2024 BY OFFENCE

The MLA Department also drafts MLA requests (issued by the Court) to other jurisdictions at the behest of the Royal Gibraltar Police and HM Customs. The number of outgoing MLA requests have increased significantly since 2018 and reflects an increased number of investigations by the LEAs.

	2019	2020	2021	2022	2023	2024	TOTAL
No. of Requests sent	4	17	16	10	10	9	66

TABLE 7 - NO. OF MLA REQUESTS SENT

The types of offences for which assistance from other jurisdictions was sought is in line with Gibraltar's risk, that being fraud followed by money laundering.

	2019	2020	2021	2022	2023	2024	TOTAL
Money Laundering	1	9	1	3	4	5	23
Fraud	2	5	6	3	5	0	21
Robbery/theft	0	2	1	0	0	0	3

	2019	2020	2021	2022	2023	2024	TOTAL
Murder/GBH	0	1	2	0	0	0	3
Drug Trafficking	1	0	1	3	1	1	7
Rape	0	0	1	0	0	0	1
Sexual assault	0	0	1	0	0	2	3
Assault	0	0	3	0	0	0	3
Driving offence	0	0	0	1	0	0	1
Forgery	0	0	0	0	0	1	1

TABLE 8 - TYPES OF OFFENCES FOR WHICH ASSISTANCE FROM OTHER JURISDICTIONS WAS SOUGHT

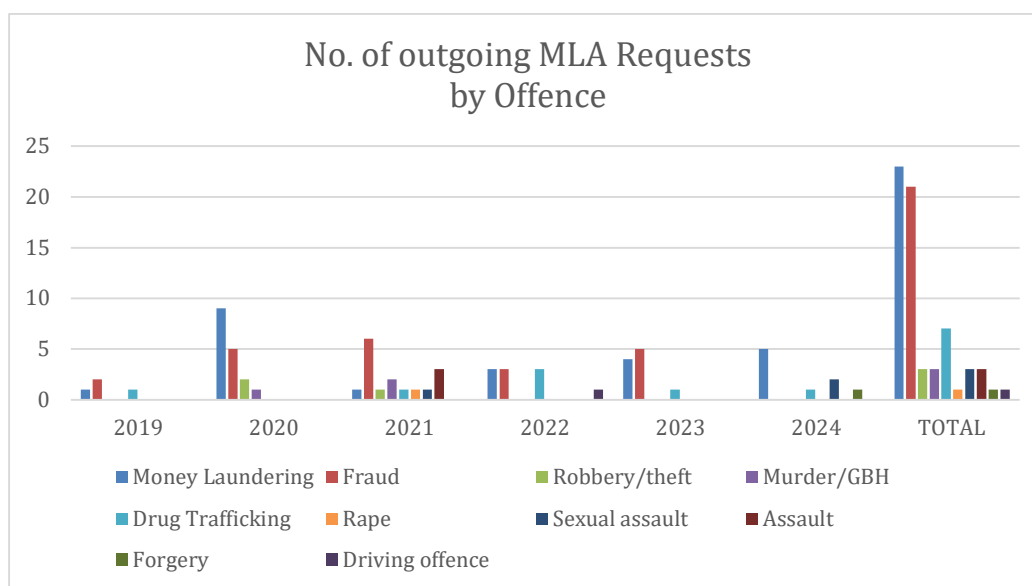


FIGURE 3 - NO. OF OUTGOING MLA REQUESTS

6.2 Organised Crime Groups

The proximity to Organised Crime Groups (OCGs) that operate in the Campo de Gibraltar has already been touched upon (see 4.1) and already featured in the previous iterations of the NRA.

Over the last few years Gibraltar has witnessed how these OCGs are increasing their influence and activities in Spain and how Spanish law enforcement agencies have been taking a more proactive approach to the detection, disruption and prosecution of their activities. Many actions by Spanish law enforcement agencies have also seen close liaison and cooperation with Gibraltar Law Enforcement Agencies in both Spain and locally.

It is therefore no surprise to note that as OCGs grow their activities and spheres of influence they may wish to use Gibraltar either as a placement location for their funds or even by way of integration and layering stages using Gibraltar based business, products or services for their laundering activities. There could also be a risk of OCGs seeking to increase their recruitment activity in the Campo de Gibraltar area and be extension into Gibraltar

It would be unlikely that OCGs themselves would seek to use Gibraltar as their primary ML jurisdiction, as this is still predominantly Spanish based, but the threat is centred on the individuals who work for these groups who may wish to spend the proceeds of their criminal activities in Gibraltar. The amendments over the last couple of years to the Petroleum Rules

effectively eliminated Gibraltar's role as a small logistical support hub for fast launches refuelling off Gibraltar waters. However, the existence of such offences prior to this highlights our vulnerability to (and local footprint of) such OCGs.

There is no evidence to support that OCG operations in Spain are being used for TF purposes but because their activities are, to a large part, associated with North Africa there are no guarantees that profits from these illegal activities are also not being used for TF activities and as such the private and public sector need to be aware of these risks.

Organised Crime Groups and the link with State Actors

State actors using criminal networks pose a threat to national security interests. Globalisation and a multipolar world order have created an environment where state actors increasingly use transnational criminal networks and other non-state actors to advance their interests. These activities include circumventing sanctions and export controls through complex ownership structures that obscure the true end-users. For example, state actors might employ front companies registered in jurisdictions like Gibraltar, which appear to comply with regulations but do not engage in significant profit-driven activities.

Recent research highlights the complex national security threats posed by OCGs, particularly those operating transnationally. The interconnection of criminal activities such as corruption, espionage, sabotage, and subversion with recent geopolitical developments presents a substantial risk. Financial and non-financial institutions must recognise and address this link to mitigate any vulnerability.

Driven primarily by financial incentives, the rise of cyber mercenaries highlights the shift of traditional illicit activities into the digital era. These mercenaries, often hired by state actors for specific operations, lack political or ideological ties to their clients. This detachment allows them to efficiently bolster resources where needed, but their lack of loyalty and the absence of control over them pose significant challenges when trying to link them to state actors.

6.3 Tobacco

Many "homegrown" Spanish Organised Crime Groups (OCGs) trace their origins back to illegal tobacco activities. This includes the production and distribution of counterfeit tobacco within Spain, as well as the unlawful importation of tobacco into Spain without paying the required import and other duties. The latter involves large volumes being imported from European countries in containers.

To a lesser extent, tobacco from Gibraltar constitutes a small volume, mostly eliminated with the discontinuation of fast launch activities in the 1980s and the implementation of stringent anti-smuggling legislation governing the storage, transportation, and possession of tobacco in Gibraltar. The control measures over tobacco wholesalers and retailers, along with the efforts of HM Customs during this period, have significantly reduced attempts to export large quantities of tobacco. Gibraltar has one of the strictest legislations governing tobacco products. This legislation regulates the licensing, sale, storage, and transportation of tobacco and grants the Collector of Customs the authority to impose any conditions deemed necessary or expedient on the retail and wholesale licenses he issues.

OCG activities persistently concentrate on tobacco distribution in Spain, with a continuing market for tobacco purchased in Gibraltar and transported across the border by frontier workers and day trippers, representing the majority of tobacco sales in Gibraltar. Although Gibraltar sells a considerable amount of tobacco, much of it ending up in Spain, the importation by Spanish nationals of amounts less than €15,000 is not considered illegal

under Spanish law. This legal threshold, combined with the price differential, sustains the market for Gibraltar-based tobacco products.

The Brexit agreement between the Governments of Gibraltar and Spain establishes a formal price differential, ensuring that Gibraltar will not undercut the retail price of Spanish tobacco by 32%. This fixed price differential aims to prevent OCGs from exploiting price differences. Additionally, Gibraltar's government adheres to the content and rules on traceability of cigarettes to eliminate illicit trade in tobacco products, following the objectives of 'The Protocol to Eliminate Illicit Trade in Tobacco Products' (Seoul Protocol).

The tobacco industry is acknowledged as a cash-intensive business, making it susceptible to exploitation by criminals due to its attractiveness and perceived security. It serves as a viable option for concealing illicit proceeds of criminal activities, presenting an uncomplicated means to obscure the origins of illegitimate funds.

Tobacco products are predominantly purchased by Spanish nationals in Euros, contributing to the high cash volumes in Gibraltar and the surplus of Euros in the economy. The existence of such large cash volumes poses a money laundering risk, and vigilance is crucial to differentiate between legitimate cash sales of tobacco and potential attempts by OCGs to control Gibraltar-based tobacco retailers and wholesalers.

HM Customs has implemented a requirement for both new applications and the renewal of wholesale and retail licences. Applicants must now furnish the Collector of Customs with a Certificate of Compliance from the Income Tax and a Certificate of Good Standing from Companies House.

6.4 Drug Trafficking

Over recent years the activities of OCGs have expanded to cover not just cannabis imports into Spain from Morocco but now firmly established as the main importers of cocaine and amphetamines into Europe, mainly via the port of Algeciras.

Cannabis imports from Morocco to Spain have traditionally used fast launches and almost always skirt BGTWs evading arrest by HM Customs and the Royal Gibraltar Police (RGP) seaborne patrols. Both LEAs continue to cooperate with their Spanish counterparts to pursue and arrest any fast launches that do stray into BGTWs. Recent prohibition by Spain on the operation of fast launches has already had an impact on this activity, although still the preferred method, and is seeing OCGs choose alternative methods through which to import Cannabis into Spain.

Other drugs, mainly cocaine is being imported via containers, through the port of Algeciras, the complex nature and volumes of freight being handled via the port makes detection difficult. As recent Spanish law enforcement cases have shown, OCGs tend to have insiders placed within the port to provide intelligence and to facilitate the smuggling operations.

As with tobacco there is no evidence to support a view that OCGs are making use of Gibraltar based businesses, products or services in a systemic manner to launder the proceeds of crime. However, their physical proximity means that businesses must be wary of attempts to buy or rent properties or purchase high value goods (usually in cash and in Euros) as a means to launder the proceeds.

Drug trafficking is the third highest predicate offence for which MLA is sought. Between 2019 and 2023, 31 requests out of 275 (11%) were made in connection with drugs offences. Of those, the majority sought evidence from e-money institutions (regarding pre-paid card, crypto-wallets, etc) (15). The remainder related to seeking evidence from: gambling operators (7), evidence held by LEAs (4), banks (2), company records (1) and 2 were for service of documents.

6.5 Fraud

Fraud is the most prevalent predicate offence for which international cooperation is sought from Gibraltar (42.5% of requests received), the second highest predicted offence indicted locally in SARs and the third most common predicate offence investigated by law enforcement.

Those on which Gibraltar's cooperation was sought are transnational in nature (i.e. committed outside of Gibraltar but the proceeds laundered in one way or another in Gibraltar). The nature of Gibraltar's economic activity, a regional financial centre, exposes Gibraltar to this type of offence.

The term itself covers a variety of actual offences (see Crimes Act <https://www.gibraltarlaws.gov.gi/uploads/legislations/crimes/2011-230.pdf#viewer.action=download> Sections 415-428) including;

Fraud

Offence of fraud.

Fraud by false representation.

Fraud by failing to disclose information.

Fraud by abuse of position.

Possession etc. of articles for use in frauds.

Making or supplying articles for use in frauds.

Obtaining services dishonestly.

Offences akin to fraud

False accounting.

False statements by company directors, etc.

Suppression, etc of documents.

Dishonestly retaining a wrongful credit

6.6 Cyber enabled Fraud

Fraud is increasingly characterised by its cross-border and cyber-enabled nature. Since most offences go unreported to the Royal Gibraltar Police, measuring the scale of cyber-enabled fraud (CEF) is currently very challenging. Notwithstanding, CEF has increased significantly internationally, with many jurisdictions reporting consistent growth in recent years. This transnational organised crime is characterised by well-structured organised criminal syndicates with specialised sub-groups, including those focused on money laundering, often operating across different jurisdictions.

These groups are linked to other criminal activities such as human trafficking, and proliferation financing associated with the Democratic People's Republic of Korea (DPRK). The variations of fraud are very broad and include Business Email Compromise, phishing techniques, social engineering, online trading/trading platform fraud, online romance fraud, and employment scams.

Criminals use the cyber domain to gain sensitive personal information through phishing attempts, often pretending to be a company to trick victims into using malicious websites or installing malware on their devices. These phishing attempts can target a wide range of individuals simultaneously, leading to identity theft, where criminals gather enough information to impersonate victims and commit fraud. Personal details can be used to obtain documents like passports or driving licenses, open new bank or credit card accounts, or take over existing accounts. Additionally, criminals exploit the internet for intellectual property fraud, creating counterfeit goods to sell online, setting up fake retail websites, or streaming content illegally.

The money laundering process involves networks that include money mules, shell companies, legitimate businesses, and various financial institutions such as banks, payment and remittance providers, and VASPs. Criminals employ diverse money laundering techniques, such as the use of cash, trade-based money laundering and unlicensed services to obscure the financial trail. Vulnerabilities in fintech products and non-traditional sectors like e-commerce are also targeted.

According to a recent FATF report, written in partnership with the Egmont Group and INTERPOL, digitalisation has enabled criminals to enhance their illicit activities' scale, scope, and speed, using tools to deceive victims and launder proceeds rapidly, often exploiting virtual services and social media to recruit money mules and set up foreign accounts.

6.7 Money Laundering / Proceeds of Crime

Money laundering/Proceeds of crime offences are the second most common form of predicate (17% of MLA requests received relate to or include money laundering) on which co-operation from Gibraltar is sought indicating that Gibraltar may be being used to launder the proceeds of crime through products and services even though the underlying offence was not committed in Gibraltar.

6.8 Bribery & Corruption

The highest threat arising for bribery and corruption arises from contact with politically exposed persons (PEPs). This is particularly significant when those PEPs, as well as their close families and close associates, have a connection with a country with a high propensity to bribery and corruption.

The only two sectors whose SARs indicate bribery and corruption are the TCSP and Banking Sectors who have only made a total of 36 SARs in the last six years. Between 2019 and 2023, only 4 requests out of 275 (0.01%) have been in connection with bribery and corruption. This does not indicate a prevalence of this offence in Gibraltar but would be commensurate with the establishment of legal structures and banking products used to conceal the benefits.

Importantly, though there is a need to distinguish the risk of domestic PEPs and those that are derived from those higher risk jurisdictions. At onboarding, and throughout the business relationship, firms must apply enhanced due diligence measures and transaction monitoring on those accounts as well as senior management approval and oversight over the business relationship. Gibraltar is not a jurisdiction where bribery and corruption of prominent persons prevails so the risk is directed to overseas PEPs who may use Gibraltar based products and services.

The TF risk for this offence is not considered significant.

6.9 Cash & Cash couriers

Gibraltar operates predominantly as a cash economy, primarily influenced by various factors. The significant presence of frontier workers, who receive their wages in cash weekly, contributes to this trend. Additionally, tourist spending is largely conducted in cash, and the sale of retail tobacco, which comprises a substantial portion of transactions, is almost exclusively cash based.

Most of the cash that enters Gibraltar through the land frontier is not destined for financial institutions but for the purchase of tobacco. The purchase of tobacco products in Gibraltar is not a criminal activity but is subject to stringent measures in pursuant to the Tobacco Act 1997. Gibraltar is the only jurisdiction in the world to impose specific limits on the amount of tobacco an individual can have on their person or vehicle:

- 1,999 cigarettes (10 cartons minus 1 cigarette) anywhere in Gibraltar without a specific licence.
- 600 cigarettes (3 cartons) in designated Special Zones.
- 200 cigarettes (1 carton) in the area immediately next to the land frontier.

To have larger quantities than these amounts without a licence issued by the Collector of Customs, would make it an offence in Gibraltar.

CASE STUDY: Tobacco in Gibraltar

Gibraltar maintains a price differential on tobacco products of no more than 32% with the equivalent product bought in Spain. This is due to the imposition of different customs duties imposed by Gibraltar and Spain. The price differential on tobacco products is governed by a post-BREXIT bi-lateral MOU. The importation of tobacco into Spain, with a total value of less than €15,000, without the payment of Spanish import duties, is treated as an administrative issue and not a criminal matter in Spain. There are four main avenues accounting for Gibraltar's high tobacco sales.

Firstly, the large number of day-trippers which most of them who return to Spain, will buy commodity items where there is a price differential in which tobacco is one of these products. Their preferred method of payment to purchase these commodities is cash.

Secondly, Gibraltar is host to approximately 10,000 to 14,000 trans-frontier workers, working in the construction, hospitality or care sectors. Most of these are paid in cash and generally in pounds sterling. As their expenditure is in Euros there is a need to convert their earnings into Euros. Larger construction companies have arrangements with MSBs where the weekly wages are wired to the MSBs and are forwarded the wage slips for each employee. The employee then turns up at the MSB and withdraws their wages from the MSB in Euros. There is an established network of persons connected with OCGs in the neighbouring Spanish city who proactively seek person to bring across the frontier one or two cartons at a time. The tobacco courier would then make around €3 per carton which if done daily can be a substantial increase in an individual's wages. Therefore, many trans-frontier workers engage in this activity, whereby they will stop at a tobacco retailer and buy one or two cartons on their way home and drop them off once they cross the frontier. These purchases are made in cash but there is no importation of cash into Gibraltar.

Thirdly, another group of people who purchase tobacco products in Gibraltar are more closely connected to Spanish OCGs. With a youth unemployment rate of over 60% in the neighbouring Spanish city, low prospects for economic and social advancement, this makes for the right environment for OCGs to offer easy cash to a large population of La Linea De La Concepcion's population. This group of people will seek to enter Gibraltar, sometimes multiple times in a day, to purchase an entire master case or two of cigarettes in cash and in Euros from a tobacco retailer. Every time a master case is taken across, the courier will collect €3 per carton x 50 cartons (number of cartons per master case) i.e. €150 for what is a little risk of being caught by the Spanish authorities, with little consequence. These individuals will then conceal the cigarettes bought on their person or vehicle to transport them into Spain. The frequency with which this operation is conducted means that every time they cross the frontier, they do so with less than £2,000 or equivalent in another currency on their person to which they can provide a plethora of explanations as to the legitimacy of the cash. This makes it very difficult for an officer to seize cash.

The fourth group of persons purchasing tobacco are the ones which use boats/vessels to export tobacco in larger quantities from Gibraltar's shoreline to Spain. Here, more than a single master case will be bought by individuals, collected or stored in a location and subsequently loaded onto a vessel. The individuals may only cross the frontier with sufficient cash to purchase a master case, below any reporting threshold that may exist in Spain for the export of cash.

HM Customs (HMC) employs the following strategies to mitigate cash flow issues. HMC enforces additional controls at the land frontier, employing measures such as cash-detection dogs, to identify and prevent the entry of cash in anti-smuggling operations. These measures contribute to the authorities in Gibraltar maintaining oversight over cash that may be intended for inclusion in the Gibraltar financial system. Using intelligence, the experience and training of officers on cash detections and the Automated Number Plate Recognition (ANPR), HMC conducts targeted stops and searches at the land frontier. In intelligence led cases, where cash is believed to be imported over the stipulated threshold found within POCA, a prior approval is obtained from the Magistrate's Court through the provisions found within the same enactment in order that individuals and vehicles can be targeted and searched.

The land frontier with Spain is 1.2km long with a policed/patrolled fence running along it. All movements in and out of Gibraltar by land, are controlled by HMC through a pedestrian/vehicle entry point and separately through a commercial gate for goods.

HMC officers are present for every flight that lands in Gibraltar, be it commercial or private. These officers have access to the Advance Passenger Information System (APIS) which is used to obtain personal data from suspects and determine travel patterns through the airport.

HMC has a maritime presence at sea 24/7 to cover the 12km coastline. There are 4 reliefs comprising of 8 officers each and they work on a 12 hour shift. They also patrol the private and public marinas within the jurisdiction. There is a "Marine Section Operational Agreement" with the Royal Gibraltar Police and the Gibraltar Defence Police, which ensures co-operation at sea. The co-ordination is done by Windmill Hill Signal Station, whose purpose is to ensure the security of Gibraltar by reporting all unauthorized arrivals of vessels.

Officers are instructed and trained on cash declarations and seizures of cash which allows them to understand the difference between the powers afforded to them by the Imports and Exports Act 1986 (for cash declarations) and the Proceeds of Crime Act 2015 (for Cash Seizures). The training also creates an awareness of the links that exists between both pieces of legislation if there is doubt to either the provenance or the intended use of the declared cash. Training has also been provided to Shipping Agents on cash declarations. Whenever there is a cash detection at any entry points a Financial Investigator will attend and assist the officers, and subsequently a detained cash investigation under POCA will be conducted by that investigator.

HMC has also signed a Memorandum of Understanding with the Borders and Coastguard Agency on how to handle the cash detected by the latter agency whilst conducting security checks at the airport during persona and personal luggage searches including the use of x-ray equipment.

This is indicative of the deterrent effect of the successfully deployed measures against the importation of large volumes of cash. HMC are mindful of the fact that OCGs are consequently deploying more sophisticated tactics to import illicit cash without detection and are adapting their modus operandi to a more intelligence-based approach.

The following statistics show the number of searches conducted at these entry points in which restricted/prohibited imports and cash would have been searched for would there have been grounds for it.

<i>Year</i>	Average No. of Searches (Individuals/Vehicles) per Month
2020	1900; (139 average during the months of lockdown)
2021	1800
2022	1900
2023	1904
2024 (Jan – Mar)	2645

TABLE 9 - AVERAGE NO. OF SEARCHES (INDIVIDUALS/VEHICLES) PER MONTH

As with commercial vessels, all yachts, pleasure crafts entering British Gibraltar Territorial Waters (BGTW) are also bound to declare cash held in excess of €10,000. All commercial vessels coming alongside at Gibraltar are physically cleared/boarded (but not necessarily searched) upon arrival. Below are the number of such vessels being searched for restricted/prohibited goods and cash.

<i>Year</i>	No. of Searches on vessels
2020	38
2021	18
2022	45
2023	33
2024 (Jan – Mar)	14

TABLE 10 - NO. OF SEARCHES ON VESSELS

In addition, Gibraltar has legislation requiring all yachts/pleasure crafts arriving in BGTW to make a crew, passenger and stores declaration. The prescribed form also makes provisions to declare cash. The electronic system requires every declaration to be cleared by HMC. The number of vessels arriving in Gibraltar and submitting declarations are as follows:

<i>Year</i>	No. of Yacht Declarations
2019	1754
2020	734
2021	753
2022	1739
2023	859
2024 (Jan – Mar)	109

TABLE 11 - NO. OF YACHT DECLARATIONS

The requirement to declare cash is not limited to amounts of €10,000 or above. Where the cash has been checked by HMC officers, all amounts have been declared correctly.

Gibraltar has maintained its cash declaration system at its external frontier points, despite its exit from the EU, for any amounts of cash exceeding €10,000. All declarations submitted are checked by HMC officers and to date there have not been any false or non-declarations found. In the past years HMC has received the following number of declarations, which most are from the Shipping Industry i.e. Commercial Vessels.

<i>Year</i>	No. of Cash Declarations
2019	193
2020	64
2021	64
2022	51
2023	69

2024 (Jan – Mar)
TABLE 12 - NO. OF CASH DECLARATIONS

8

In light of the relatively small crossing of cash into Gibraltar detection of substantive quantities is difficult. The table below shows the cash seizure amounts and forfeitures from 2017 to 2024 (Jan – March). Almost all of these detections have been at the land frontier with Spain. As can be seen, all but one were below €10,000.

Year	Total Cash Seizures	Total Forfeited	Total Cash Seized	Cash Forfeited	Cash Returned
2017	17	15	£2,000 and €93,577	£2,000 and €86,853	€6724
2018	11	4	€39,335	€11,075	€28,260
2019	11	7	£5,200, €145,378, \$66,300 and 220MAD	€112,999	£70, €32,360, \$66,300 and 220 MAD
2020	7	3	£93,299, €59,285 and \$3,609	£82,800, €54,935 and \$3,609	£10,500 and €4,350
2021	3	2	€14,400	€12,000	€2,400
2022	3	0	£11,250 and €19,405	N/A	£11,250 and €19,405
2023	4	1	£9,850 and €7,400	£9,850	€7,400
2024 (Jan – Mar)	1	N/A	£6,230	N/A	N/A

TABLE 13 - CASH SEIZURE AMOUNTS AND FORFEITURES)

NB: The difference in value between Cash Seized and the aggregated total between Cash Forfeited and cash Returned, is due to pending cases.

Statistics collected by the GFSC shows a large number of transactions occurring within the regulated sectors (see below). This activity is representative of the mainly non-resident client base of the institutions. A cash withdrawal from a Gib bank account at a UK ATM would show up on these statistics as an outflow of cash to the UK even though no cash has been physically transported to the UK via Gibraltar. Similarly, a cash top-up of a Gibraltar pre-paid card in another jurisdiction will show up as a cash inflow even though no cash has arrived in Gibraltar from that jurisdiction. This distortion in the GFSC data is precisely because of the accounting of transactions belonging to Gibraltar HQ firms alone and not representative of physical cash transportation in and out of Gibraltar.

	2021	2022	2023	2024
Accountants	£0	£0	£0	£0
Auditors	£0	£0	£0	£0
Banks	£372,175,254	£340,413,636	£318,160,591	£161,822,708
Bureaux	£0	£0	£0	£0
Consumer Credit	£998,067	£1,000,796	£0	£0
DLT	£0	£0	£0	£0

<i>E-money</i>	£3,236,489	£4,323,660	£1,717,510	£2,258,211
<i>Fund</i>	£0	£0	£0	£0
<i>Administrators</i>				
<i>Funds</i>	£0	£4,838,600	£7,997,702	£611,720
<i>Insurance (life)</i>	£0	£3,434,162	£0	£0
<i>Insurance managers</i>	£0	£0	£0	£0
<i>Intermediaries (general)</i>	£201,835	£0	£0	£0
<i>Intermediaries (life)</i>	£0	£0	£0	£0
<i>Investments</i>	£0	£0	£0	£0
<i>Insolvency Practitioners</i>	£0	£0	£0	£0
<i>Pension advisors</i>	£0	£0	£0	£0
<i>PPSCs</i>	£0	£1,256,159	£3,031,441	£1,101,602
<i>Regulated market</i>	£0	£0	£0	£0
<i>Small scheme managers</i>	£0	£0	£0	£0
<i>Tax advisors</i>	£0	£0	£0	£0
<i>TCSPs</i>	£0	£0	£0	£0
<i>Virtual Asset Arrangement Providers</i>	£0	£0	£0	£0

TABLE 14 - TOTAL VALUE OF PAYMENTS RECEIVED IN CASH

6.10 Trade Based Money Laundering

Although there is no current intelligence to suggest that Trade Based Money Laundering (TBML) is in any way prolific in Gibraltar, the authorities, including HMC, are aware of the potential of this becoming an issue in the future. This is mainly due to Gibraltar being a small jurisdiction with no production capacity on one of the busiest shipping lanes in the world.

Consequently, to mitigate the potential risk of exploitation of Gibraltar's trade movements, HMC prioritises the scrutiny of goods and trade flows which lend themselves to TBML. In addition to the continued upgrading of HMC's UN (UNCTAD) ASYCUDA software, relevant officers will undertake further training including World Customs Organisation training on goods classification, goods transits, risk management and post clearance declaration auditing as well as TBML specific training via the Gibraltar Financial Intelligence Unit. This will further enhance the HMC's capability to manage this potential risk.

6.11 Modern Slavery, Human Trafficking and Migrant Smuggling (MSHT)

Modern slavery is often a hidden crime involving one person denying another person his or her freedom. It includes slavery, servitude and forced or compulsory labour, and human trafficking. Gibraltar's commitment to combating modern slavery, human trafficking and migrant smuggling extends beyond punitive measures that covers support and assistance for victims. Alongside criminalising all forms of human trafficking, including harbouring and exploitation, Gibraltar's laws also contain provisions for the protection and care of victims. It is enshrined in law that it is the duty of the Government to provide the necessary resources

to ensure that individuals who may have been subjected to human trafficking offences receive immediate assistance and support as soon as there are reasonable grounds for suspicion. This comprehensive approach highlights Gibraltar's commitment to safeguarding the well-being and rights of those affected by this heinous crime, by being in line with international standards.

It is important to understand the difference between human trafficking and migrant smuggling. Human trafficking can involve various forms of coercion, including physical force, threats, deception, and the abuse of power or a position of vulnerability. A victim of human trafficking can be exploited during the journey and/or at the final destination. Migrant smuggling is a mutually agreed service, usually involving transportation and/or fraudulent documents to enter a foreign country illegally. The person being smuggled is consenting to the movement. Once this exchange is complete the person is free to make other choices.

When examining these two terms, it's important to consider Gibraltar's geographical position and vulnerability to migrant smuggling, as well as its status as an international finance centre, which also exposes it to the financing of both migrant smuggling and human trafficking. This offers Gibraltar a unique perspective on human trafficking and migrant smuggling, and its ability to coordinate intelligence effectively is crucial to combat one of the most profitable crimes in the world. There have been no instances of human trafficking reported in Gibraltar. However, Gibraltar's airport is believed to have been used as a transit point for the UK. In May 2024, a Chinese Organised Crime Group (OCG) that allegedly smuggled more than 250 Chinese nationals to the UK via Gibraltar were dismantled by the Spanish police.²

Illicit proceeds from human trafficking, including profits from victim exploitation and payments to logistics, airlines, transportation, car rental, or travel agents, often intersect with the regulated financial system. This occurs throughout the recruitment, transportation, and exploitation stages, where financial transactions inconsistent with the customer's personal use or stated business activity may occur. New figures published by the Global Coalition to Fight Financial Crime, estimates that the global illicit proceeds could be a staggering \$498 billion³.

CASE STUDY: Migrant smuggling in the Strait of Gibraltar

Gibraltar is located at the crossroads between Africa and Europe, in a strategic position along the 'Western Mediterranean route' for illegal migration. This geographical location makes it a significant point for transiting vessels with individuals seeking to cross borders illegally, often in pursuit of better opportunities or refuge. International and regional reports consistently indicate a steady increase in these offences at both regional and global levels, and this trend persists in countries that are positioned along migration routes or sharing borders with migrant source or destination countries, whether by sea or land. However, investigations into migrant smuggling have yet to uncover any instances of money laundering or other illicit financial activities involving financial services or products in Gibraltar.

Gibraltar plays a crucial role in regional efforts to combat these illicit activities and promote security and stability in the wider Mediterranean region. OCGs are fluid and agile criminal enterprises that adapt to legislative changes and to shifts in market demand. By way of example, in 2020, during a collaborative operation between the Spanish Policia Nacional and Royal Gibraltar Police targeting an OCG, 47 individuals were arrested.⁴ This group was involved in smuggling

² <https://www.gbc.gi/news/cross-border-chinese-human-trafficking-gang-dismantled-spanish-police>

³ <https://www.gcffc.org/gcffc-estimates-proceeds-from-human-trafficking-at-usd-498-billion/>

⁴ <https://www.police.gi/news/joint-rgp-policia-nacional-operation-dismantles-migrant-smuggling-organised-crime-group-297>

migrants from Morocco to Spain and several other European nations, with over 130 smuggled Moroccan nationals discovered in Spain. Each migrant smuggled from Morocco was charged between 7,000-8,000 Euros, resulting in the OCG amassing over 1 million Euros in profit. The illicit enterprise affected 18 Spanish provinces and five European countries, prompting the involvement of over 200 Policia Nacional officers and Royal Gibraltar Police officers in the operation, all under the coordination of EUROPOL. The investigation reached its climax with the execution of two search warrants at residential properties in La Linea and Gibraltar, the latter authorised by a European Investigation Order. Despite the extensive nature of this operation, instances like these remain rare, with only isolated cases detected of individuals attempting to reach Europe via boats that have ended up in British Gibraltar Territorial Waters (BGTW), due to other factors such as weather or vessel conditions.

An analysis of Suspicious Activity Reports (SARs) submitted to GFIU, primarily associated with human smuggling, suggests that OCGs employ a range of sectors and methods to launder the proceeds. These methods include the use of Money Service Businesses (MSBs), e-Money, virtual asset service providers, TCSPs and banks. Nevertheless, SARs on MSHT remain low in Gibraltar. This underreporting is consistent with other countries and is a characteristic of the type of crime. According to a EUROPOL report,⁵ the evolution of OCGs into a professionalised and flexible service represents a growing challenge for EU law enforcement agencies (LEAs). Beyond the resilient business model adopted by OCGs, there is a substantial intelligence gap among LEAs regarding the financial dimensions of MSHT.

Detecting these types of illicit financial activity proactively is therefore of paramount importance. Through Project Nexus, the GFIU conducts awareness training and provides outreach to reporting entities and offers a specific workshop on its e-learning platform, e-Nexus, focusing on the financing of human trafficking. This outreach extends to its social media platforms, contributing to the maintenance of awareness on the topic.

The GFIU has also partnered with the RGP to offer capacity building opportunities in investigating MSHT offences, aimed at enhancing interview strategies and formulating questions to gather intelligence on MSHT networks and their financing methods. These efforts contribute valuable insights into regional illicit activities.

Additionally, the GFIU has collaborated with UNODC (ROMENA) and INTERPOL to provide training on this subject in various countries, facilitating awareness-raising efforts and better understanding of the latest typologies.

The risk of MSHT is considered to be low.

6.12 Illegal Wildlife Trade

The illegal wildlife trade (IWT) has become one of the most profitable illegal enterprises that is orchestrated by sophisticated transnational organised crime groups capitalising on the staggering USD 23 billion that is generated annually, fuelled by an unquenchable thirst for consumption, social status, and traditional remedies. This makes criminal networks exploit systemic vulnerabilities with a low-risk, high-profit approach.

Although there is no universally accepted definition of the term, the United Nations Office of Drugs (UNODC), defines the IWT as the illegal trade, smuggling, poaching, capture, or collection of endangered species, protected wildlife (including animals or plants that are subject to harvest quotas and regulated by permits), derivatives, or products thereof.

⁵ EUROPOL, "The THB Financial Business Model: Assessing the Current State of Knowledge July 2015", https://www.europol.europa.eu/cms/sites/default/files/documents/europol_thb_financial_business_model_2015.pdf

Located at the crossroads between Africa and Europe, Gibraltar has a vibrant bunkering business with vessels regularly stopping on transit to other ports of call. Despite its strategic location, it has not detected or seized any wild animals or plants in recent years. Gibraltar's finance centre has a key role to play to combat this crime and raising awareness on it will be crucial to be able to identify how criminals are able to exploit formal banking systems to launder their illicit funds.

IWT has shown to have significant ties to corruption and transnational organised crime groups, both of which are key priorities in GFIU's efforts to combat economic crime and the financing of terrorism. Consequently, to enhance capacity and demonstrate Gibraltar's global commitment to tackle the IWT, the Gibraltar Financial Intelligence Unit (GFIU) signed a memorandum of understanding (MoU) with the Department of the Environment in May 2020 which formalised the relationship between the two units. The MoU seeks to strengthen the international efforts against IWT and the financing of such trade. It establishes agreed protocols whereby information can be exchanged within the parameters of Gibraltar's legislative framework and be able to receive scientific support or advice.

Furthermore, the GFIU collaborates with HM Customs on a regular basis, facilitating the exchange of information and providing training opportunities to Customs officers through e-learning systems to better understand the illicit financial flows generated by IWT. Additionally, HM Customs have sourced specific World Customs Organisation 'Convention on International Trade in Endangered Species of Wild Fauna and Flora' (CITES) training to bolster proficiency in the classification of species and the detection of IWT to ensure a more robust approach to the enforcement of pertinent legislation.

According to the FATF, both small-scale and large-scale criminals engaged in the IWT frequently use shell and front companies to obscure payments and launder the profits from their illicit operations⁶. Criminals primarily use shell companies to facilitate the transfer of value among syndicate members, between buyers and sellers, or to retain assets. Additionally, criminals use front companies, which typically engage in legitimate business alongside illegal activities, to facilitate the transportation of wildlife and to blend lawful and unlawful proceeds, thereby concealing the transfer of value.

Although the risk of IWT is considered to be low, Gibraltar's finance centre has a key role to play to combat this crime and raising awareness on it will be crucial to be able to identify how criminals are able to exploit formal banking systems, e-money payments and front companies to launder their illicit funds.

7 Sectoral Assessments

7.1 Banking

Gibraltar hosts a small Banking sector comprised of nine credit institutions. The sector is comprised of private banking institutions, locally incorporated subsidiaries of foreign banks, two branches and three Gibraltar-based institutions.

All banks are subject to supervision by the Gibraltar Financial Services Commission (GFSC). In 2020, the GFSC undertook an AML/CFT/CPF thematic review of the banking sector,

⁶ Money Laundering and the Illegal Wildlife Trade, FATF, June 2020, (<https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Money-laundering-and-illegal-wildlife-trade.pdf>)

publishing the cross-sectoral findings identified by way of its onsite inspections within its [Banking Sector Thematic Review Report](#). Following the completion of the sectoral thematic review, all banking institutions have since been subject to further onsite inspections by the GFSC. The standard of compliance against AML/CFT/CPF related requirements across the sector is considered generally high, with minor to no deficiencies identified in the case of the majority of banks as at the most recent reviews.

Number of banks licensed in the country, of which:	9
Have branches and subsidiaries abroad	1 - United Kingdom
Foreign owned	8
Number of foreign banks which operate in the country through establishment of a branch / branches	2
Total deposits	£8,720,471,957
Total number of clients	78,780

TABLE 16 - MATERIALITY OF BANKING SECTOR AS AT 31 DECEMBER 2024

The banking sector represents the majority of transactions issued to and received from jurisdictions deemed as posing a higher risk, in terms of both transactional volume and value. Data provided by the credit institutions in the Annual Financial Crime Return submitted to the GFSC shows that both the number and value of transactions received from or issued to high risk jurisdictions by the banking sector has increased since 2020. This increase is commensurate with the overall growth in transactional activity identified in the sector and is therefore considered expected given the key role that credit institutions play within the financial system.

Activity/Risk of counterparty	Low	Med Low	Med High	High
Correspondent banks with which the firm holds relationships	41	29	1	2
No. transactions received from	1,322,390	37,324	35,454	7661
No. transactions issued to	1,699,026	39,592	92,476	19,481
Funds received from	£24,706,958,688	£2,590,449,727	£1,584,091,202	£679,289,951
Funds issued to	£27,812,728,027	£4,031,368,654	£1,566,054,153	£273,201,700

TABLE 17 - BANKING DATA FOR 2024

From 2021-2024 the banking sector has been the third-highest reporting sector in terms of SARs, representing approximately 6.89% of the total SARs reported in 2024 (16.49% of SARs reported when excluding the gaming sector). This is despite the low number of credit institutions and customers in comparison with other larger sectors. This further demonstrates the high standard of AML/CFT/CPF controls applied within the sector. The predicate offences associated with the reports made by the sector predominantly relate to suspicions of fraud and ML, followed by tax crimes and robbery/theft.

Deposit-taking

Deposit-taking constitutes an essential foundation of the products and services offered by the banking sector in Gibraltar. The primary financial crime-related threat associated with deposit-taking institutions is that they may be used by perpetrators to place illicit proceeds into the financial system in order to obfuscate their illicit origin. Terrorist actors, as well as their supporters or facilitators, may also potentially deposit funds from either legitimate or illegitimate sources into a credit institution with a view to accessing those funds for purposes associated with potential acts of terrorism.

Internationally, OCGs (as well as their relatives or close associates) are known to use deposits-on-account for the purposes of disguising criminal proceeds. Law enforcement authorities internationally have reported on frequent use of this method, as it presents one of the most frictionless means of integrating illicit funds into the financial system. The complexity of a particular case can differ significantly between instances and may involve a chain of multiple linked complex operations, warranting an in-depth understanding of the potential threats and vulnerabilities faced by institutions.

Unwitting customers of banking institutions may also be coerced, lured or deceived into moving assets on behalf of a criminal actor using their own personal accounts, acting as a “money mule”. This is typically achieved through a variety of means including cybercrime, phishing, identity theft and online scams. “Bridge accounts” (i.e. a temporary or intermediary account used to facilitate a specific financial transaction) also pose a potential money laundering threat, given their ability to enable the cross-border movement of assets and increase the complexity of a financial transaction. It is important to note that use of both the “money mule” and “bridge account” mechanisms to facilitate financial crime has not been identified as having occurred within Gibraltar and is therefore, not considered a material risk.

In the case of TF, international experience highlights that terrorist groups and actors frequently use deposits-on-account to introduce cash into banking institutions and ultimately withdraw assets for the purpose of funding terrorist activities. This mechanism continues to represent one of the simplest methods to introduce money into the financial system. Given the low value of funds required to potentially facilitate a terrorist act, detecting such activity often poses an increased level of difficulty (particularly in cases where the origin of the assets in question is legitimate). As per the GFSC’s supervision, the standard of transaction monitoring controls applied by local credit institutions is typically high. There have also been no identified instances where deposits-on-account have been used to facilitate such purposes. The risk posed is therefore considered to be low.

In relation to the issuance of funds to conflict zones, the level of TF risk presented by deposits-on-account is considered decreased, on the basis that terrorist actors (and their associates) typically favour the use of money value transfer services or e-money products, given their increased ease of use and accessibility. This is corroborated by the data received by way of the GFSC’s Annual Financial Crime Return, where the value of transactions issued to or received from known conflict zones represents <0.33% of total transactions undertaken by the banking sector in 2023.

YEAR	Proportion of transactions issued to or received from conflict zones (number)	Proportion of transactions issued to or received from conflict zones (value)
2021	0.01%	0.07%
2022	0.03%	0.05%
2023	0.40%	0.33%

2024	0.24%	0.64%
------	-------	-------

TABLE 18 - CONFLICT ZONE TRANSACTIONS WITHIN THE BANKING SECTOR

Corporate banking customers can expose credit institutions to ML, TF & PF risks on the basis that they can be established in a manner that obfuscates the true nature and identity of the ultimate beneficial owner(s). This is particularly relevant where trade-based transactions are linked to jurisdictions with less stringent AML/CFT/CPF regimes that do not require a high standard of transparency. For this reason, a complex ownership structure involving multiple layers of ownership across different jurisdictions can often be considered a red flag indicator. As per the GFSC's supervision, no instances have been identified where a credit institution has failed to meet its statutory obligation of identifying the ultimate beneficial owner(s) of a corporate customer.

Corporate customers which are cash-intensive businesses pose an increased level of ML risk to banks on the basis that perpetrators operate or use cash-based business to commingle illegally obtained funds with cash generated legally by the business. Through its supervision, the GFSC ensures that economic activity identified as consisting of a high propensity of cash is considered a high risk factor that may warrant the application of additional mitigatory controls. As part of the application of due diligence measures, all financial institutions are required to identify (and where necessary in line with the level of risk posed, verify) the source of funds and wealth of a corporate customer, as well as that of the ultimate beneficial owner(s) of that customer. This is to ensure that the fiscal activity of a corporate customer is in line with its economic profile and to mitigate the risk of a beneficial owner's ability to transmit illicit funds through the legitimate business operations of the corporate.

Corporate due diligence documentation required to be submitted to credit institutions as part of a business relationship are also at risk of potential forgery/falsification. Additionally, the increasing role of intermediaries and facilitators in adding to the complexity of a financial transaction for the benefit of organised crime groups also increases the inherent risk associated with these products. The high standards of AML/CFT/CPF controls applied by Gibraltar credit institutions mitigate these risks substantially.

The carrying out of a terrorist act typically involves the use of small amounts of funding. Maintaining a terrorist organisation itself, however, may require significantly higher levels of funding to facilitate the receipt of financial support and pay out of the living costs of its members (e.g. in the form of wages or rent payments). Corporate customers (with legitimate or illegitimate economic activity) may therefore be susceptible to be used for such purposes, although it is typically considered that perpetrators do not have sufficient expertise to exploit these services on a large scale. As per the data received by way of the GFSC's Annual Financial Crime Return, the number of corporate banking customers either established or active in, a high risk or conflict zone jurisdiction, is considered negligible (>3%). The level of residual TF risk associated with corporate banking services is therefore, considered low.

In recent years, the Gibraltar corporate banking sector has contracted. As identified by way of the GFSC's Annual Financial Crime Supervisory Return, the total number of corporate banking customers has decreased by approximately 60% since 2020; this is likely due to the impact of Brexit and the Covid-19 pandemic. In accordance with the data for the 2024 reporting period, corporate entities represent approximately 4.12% of customers of Gibraltar credit institutions. This is further demonstrated in the figure below which distinguishes between the proportion of newly onboarded corporate and individual customers per year. The level of risk posed by corporate banking services is therefore considered to have decreased.

Broker Deposits

There are several scenarios where perpetrators can commit abuses related to institutional investment. These include activities relating to fraud, market abuse, the use of investment to justify criminal proceeds as profit, predicate investment fraud, and placement of proceeds using specialised high-return investments. The increasing role of facilitators and intermediaries in ML highlights a potential increase in exposure to such threats, although significant levels of technical expertise are required in order to execute them. While large volumes of funds can be obtained through these processes, it is not considered easily accessible and may not be financially viable (depending on the terms and quality of the investment).

The role of intermediaries is often key in creating complex and opaque financial structures in an effort to hide the proceeds of criminal activity. Credit institutions are often the first barrier that could act in preventing illicit funds from entering the financial system and mitigating the inherent ML risk.

The TF threat surrounding institutional investment primarily relates to scenarios in which large sums of legitimate funds are invested for the purpose of financing terrorism. This is dependent on the nature of the terrorist activity in question, however, this is not an attractive means when considering the typical use of small amounts.

In practice, there are only a small number of brokerage accounts held at Gibraltar credit institutions. This, together with the high typical standard of compliance maintained within the sector considerably mitigates the potential vulnerability.

Lending Activities

Mortgage Credit & High Value Asset-Backed Credits

Criminals disguise and invest the proceeds of crime by way of real-estate investment. The proceeds are used for deposits, repayments and early redemption.

Mortgage credit is a method frequently operated by organised crime groups, using false documentation and third-party involvement in mortgage structures to hide the true beneficiary. This method aids criminals in owning multiple properties and concealing their assets' scale. This method is still used for the integration phase (mostly for lower amounts as it does not require sophisticated operations). However, it is more often used alongside complex ownership chains for real estate.

The inherent risk can be high because of the link with the real estate sector as criminal organisations prefer to launder the proceeds of their activity by means of high-value transactions. Real estate agents are supervised by the OFT for AML/CFT purposes, which also serves as a mitigating factor.

Terrorist groups use (medium/long-term, low-interest) high-value asset-backed credit/mortgage loans to fund potential terrorist activities. Loans are taken out for relatively high amounts to access funds that are untraceable as long as the money is not transferred.

The assessment of the terrorist financing threat related to mortgage credit shows that terrorist groups find it difficult to use mortgage credit for funding due to the need for a relationship with a complicit third party. There have been no instances of this activity identified locally, and the level of risk posed is therefore considered low.

Business Lending

Internationally, illicit actors are known to use business loans to repay with illicit funds and sometimes employ credit cards to make the source of funds seem legitimate. Loans give criminal funds an appearance of legitimacy.

The assessment of the money laundering threat within Gibraltar has identified that it is uncommon for criminals to exploit the use of business loans, which are perceived as unappealing. This is because fake loans are often part of fraud schemes (e.g. two companies take out a fake loan and use a bank to transfer funds) and so are not necessarily used for the purposes of laundering the proceeds of crime. The main risk posed by these products lies in businesses potentially redeeming these loans early, sometimes with cash from unclear sources. However, this has not been found to be a trend or typology in the Gibraltar banking sector.

Generally, worldwide, the assessment of the terrorist financing threat related to business loans shows that there have been few cases of terrorist groups using business loans to collect funds. There have been no cases of this locally, and so the TF risk in this instance is considered low.

Consumer Credit and Low Value Loans

Terrorists and organised crime groups can use short-term, low-value, high-interest loans like payday, consumer credit and student loans for untraceable funds. Loans are given for relatively low amounts, allowing access to funds. This is appealing because the sources are untraceable if the money is not transferred. They also exploit credit cards to withdraw cash, leaving a negative balance with no intention of repayment.

The assessment of the terrorist financing threat related to consumer credit and low value loans shows that terrorist groups may use this method to finance travel by foreign terrorist fighters to high risk countries. Consumer credit firms are subject to GFSC supervision, which somewhat mitigates the risks associated. The Annual Financial Crime Return data submitted to the GFSC shows that 98% of consumer credit customers are local residents and there are no consumer credit customers based in conflict zone jurisdictions, meaning the TF risk remains low.

This kind of loan can also be used to launder the proceeds of criminal activity. These products offer less money laundering potential than other financial products due to their low value, but a common international typology associated with this is that criminal organisations use them to finance the purchase of high value goods and then redeem the loans by cash. High value goods dealers are subjected to AML/CFT Supervision by the Office of Fair Trading, reducing the associated risk. Additionally, these are not typologies which have been encountered in Gibraltar and there are currently no high value goods dealers in Gibraltar, as per the definition set out in the Proceeds of Crime Act 2015, further mitigating this risk.

Private Banking/Wealth Management

Although the wealth management and private banking industry in Gibraltar is small, comprised of three institutions, it may still pose ML and TF risks. These risks primarily arise due to intricate arrangements designed to safeguard clients' wealth, involving not only corporate and trust structures but also intermediaries and advisors.

Wealth management and private banking services are particularly susceptible to the risk of being used to launder the proceeds of overseas corruption. To mitigate these risks, the Proceeds of Crime Act 2015 requires firms to apply enhanced due diligence to higher risk customers.

Instances where customers have held significant public roles in high-risk third countries should be given additional consideration to PEP-associated risks. PEPs who hold prominent public functions in Gibraltar (and their family members and close associates) are treated in the same manner under the Proceeds of Crime Act 2015 where there is no distinction in the enhanced measures required for domestic and foreign PEPs. Firms must apply more

stringent approaches in cases of higher risks, especially in relation to PEPs from countries where corruption is a higher risk. PEP customers only form 3.9% of the total customers within the banking sector as reported within the GFSC's 2023 Financial Crime Return. The total number of foreign PEPs including close associates and family members is 201 with domestic PEPs totalling 177.

The mitigation measures related to Private Banking are also in relation to the following areas:

- Many corporate clients employ complex structures so a good understanding of the nature/activity of the account and all the natural and legal persons behind the structure is required;
- Ongoing monitoring is essential to ensure account activity aligns with what was initially described during account opening; and
- Client base is smaller, which facilitates better customer knowledge, understanding and monitoring capabilities.

The GFSC conducted a thematic review of the Banking sector throughout 2020 and 2021, and firms showed a notable understanding of the ML/TF risks posed by private banking/wealth management services.

ML Threat and Vulnerability Assessment

Credit institutions continue to be exposed to a high level of ML risk, given the central role that they play within the worldwide financial sector. Despite the high standard of controls applied within the sector (as verified by the GFSC as the relevant supervisory authority), the widespread criminal intent to exploit banking products, as well as the increasing speed and volume at which transactions are undertaken, means that the sector remains at an inherently higher risk of facilitating ML.

Money laundering forms the most common grounds for suspicion upon which credit institutions have raised SARs to the GFIU. The figure below breaks down the SARs submitted by the sector in relation to the type of suspected criminality. When excluding the e-gaming sector, the reports issued by the banks represent 23% of the total SARs raised in 2023 where the grounds for suspicion was ML. This demonstrates the ongoing vulnerability of the sector to this illicit activity.

TF Threat and Vulnerability Assessment

Credit institutions continue to face significant exposure to the risk of TF due to their role in the global financial sector. The intent to exploit banking products, combined with the escalating speed and volume of transactions, keeps the sector at a heightened risk of facilitating terrorist financing. The swift and cross-border nature of these transactions is particularly attractive to terrorist actors. Despite this, the banking sector as a whole applies stringent controls to mitigate these risks, and the TF risk is generally considered to be lower. The GFSC also operates an enhanced supervisory approach for AML/CFT purposes. According to the data submitted for the 2023 Financial Crime Return, customers resident in conflict zones represented 6.77% of total customers in the Banking sector, confirming that the exposure remains low.

This assessment and conclusion are further strengthened by the low level of SARs submitted to the GFIU relating to TF. In 2023, out of the 4887 SARs submitted, none of the SARs raised from the banking sector related to suspicions of TF. TF suspicions constituted 0.10% of SARs in 2021 and 0.22% in 2020.

7.2 Trust and Corporate Services Providers

Trust and Corporate Service Providers (TCSPs) provide a wide range of services related to the establishment, management and administration of trusts, companies and other legal entities or arrangements.

The types of services offered by TCSPs in Gibraltar include:

Company Formation and Management: TCSPs assist clients in setting up various types of legal entities, such as private limited companies, limited liability companies, and partnerships.

Trust Formation and Administration: TCSPs help clients create and manage trusts - a type of legal arrangement where assets are held and managed by a trustee for the benefit of designated beneficiaries. These TCSPs ensure that trusts are structured in accordance with legal requirements and client preferences.

Secretarial and Registered Office Services: TCSPs handle administrative tasks such as the maintenance of records and filing the requisite documents at Companies House. In addition, they have the right to act as corporate secretaries on behalf of client companies. Registered office services allow for companies to have a physical presence in Gibraltar even if they are not based within the jurisdiction.

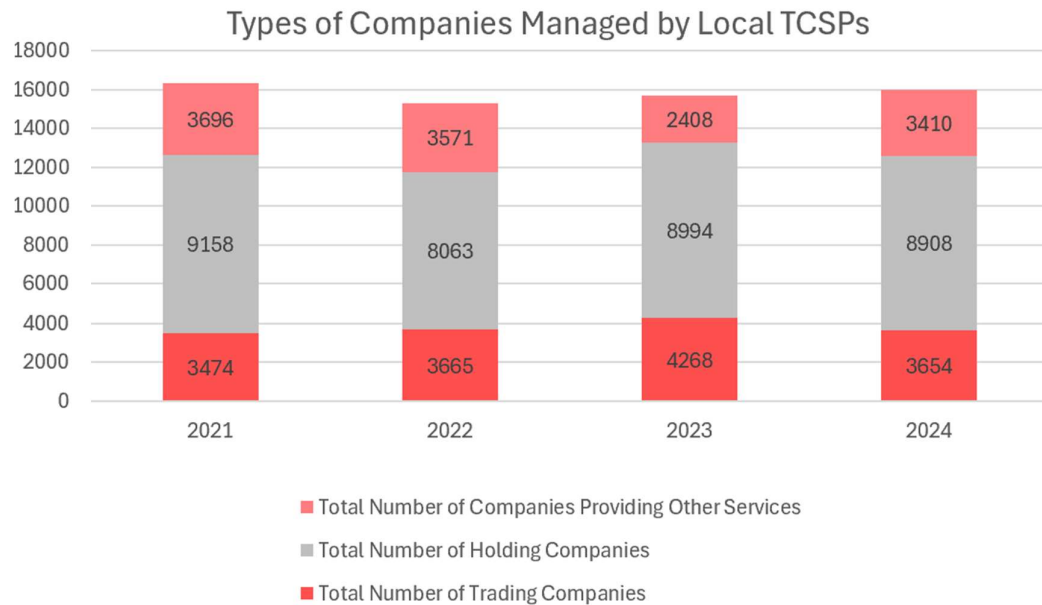
Directorship and Nominee Shareholding Services: TCSPs and its officers can serve as directors on behalf of client companies. They can also provide corporate entities to act as nominee shareholders on behalf of client companies.

Gibraltar was one of the first jurisdictions to introduce a regulatory framework for the provision of trust and corporate services which was established in 1990.

Composition and size of the TCSP Sector

Total number of entities, of which:	-
Corporate TCSPs	54
Belong to international groups	8
Number of TCSPs that prepare for or carry out transactions for a client concerning the following activities;	-
acting as a formation agent of legal persons;	54
acting as (or arranging for another person to act as) a director or secretary of a company, a partner of a partnership, or a similar position in relation to other legal persons;	37
providing a registered office, business address or accommodation, correspondence or administrative address for a company, a partnership or any other legal person or arrangement;	54
acting as (or arranging for another person to act as) a trustee of an express trust or performing the equivalent function for another form of legal arrangement;	25
acting as (or arranging for another person to act as) a nominee shareholder for another person.	37
Number of legal persons serviced	16,246
Number of legal arrangements serviced	1808

TABLE 19 - MATERIALITY OF THE TCSP SECTOR AS AT 31 DECEMBER 2024

**FIGURE 4 - TYPES OF COMPANIES MANAGED BY TCSPS**

TCSPs are authorised under the Financial Services Act 2019 and are subjected to additional sector specific regulations under the Financial Services (Fiduciary Services) Regulations 2020. These regulations outline the conduct, compliance and prudential requirements that TCSPs must adhere to. As relevant financial businesses, TCSPs are also required to comply with all relevant requirements under the Proceeds of Crime Act 2015 (POCA).

All TCSPs who wish to carry out these functions must apply to the GFSC for authorisation. During the application process, any potential applicants must meet all the requirements set out in the Financial Services Act 2019, the sector specific regulations and POCA. Applicants are subjected to robust due diligence checks in ensuring that the entity, and any individuals behind the entity including its officers and shareholders or controllers, are fit and proper and not associated with any illicit or criminal activities. The GFSC's assessment also includes an assessment of the applicant's experience and requisite knowledge to perform the regulated functions.

Individuals who provide directorship services to client companies are required to be linked to an authorised TCSP entity and must also be authorised by the GFSC in their own right in obtaining an individual company manager licence. It should be noted that once an individual ceases to be employed by the TCSP, the individual licence is also cancelled at that stage.

The requirements under POCA to which TCSPs are subjected to extend to areas such as customer due diligence, beneficial ownership, politically exposed persons, and ongoing monitoring. With 98% of all Gibraltar legal entities being managed by local regulated TCSPs, risks that are normally associated with legal entities (complex and opaque structures to hide beneficial owners) are substantially mitigated. The GFSC's supervisory plan includes verification that the requirements under POCA and the GFSC's AML/CFT Guidance Notes are being adhered to.

The overall compliance with the requirements laid out in the Proceeds of Crime Act 2015 has increased year on year by the TCSP sector. The sector has had a 40% decrease in the number of findings across the board since 2020. The GFSC continues to work with this sector to strengthen the controls, enhance compliance and raise awareness of the typologies associated with this sector.

Gibraltar currently has 55 active TCSP groups managing circa 16,246 companies and 1,808 trusts. Over 80% of these are locally incorporated entities. Gibraltar implemented a beneficial ownership register in 2017 where all companies registered within the jurisdiction are mandated by law to disclose and submit the ultimate beneficial owners of each legal entity to the Registrar.

Creation of Legal Entities and Legal Arrangements

The establishment of legal entities and arrangements enables individuals to construct intricate ownership structures that involve multiple tiers of entities spanning various jurisdictions. While these structures are often exploited for illicit purposes, they also serve legitimate functions, such as multinational corporations operating across different regions. Nominee shareholding services can serve as indicators of potential issues, but they can also function as risk mitigation tools. In the context of nominee shareholding services, they introduce an extra layer of obscurity concerning beneficial ownership, however, they also grant the TCSP more authority over the legal entity or arrangement. The AML/CFT thematic review which took place in 2018 gave the GFSC a broad understanding of the TCSP sector within Gibraltar and the threats and vulnerabilities associated with each regulated entity and these entities have been subject to an ongoing enhanced supervisory approach for AML/CFT purposes. Generally, providing only secretarial services and registered office facilities has always been viewed to present a lower risk, however, the jurisdiction takes the approach that these services can also present a higher risk on the basis that the TCSP may not have full oversight or control over the legal entity or arrangement, its transactions or activities. Therefore, the requirements under POCA apply to TCSPs in the same manner regardless of the activities being provided to the client. As part of the client onboarding process, TCSPs are required to obtain the rationale for the establishment of a legal entity or arrangement within Gibraltar. In addition, any tax advice provided to the client is requested by the TCSP to ensure the legal entity or arrangement is not being set up for the purposes of tax evasion.

The creation of legal entities and arrangements overall presents a higher risk to the jurisdiction. This is based on the number of legal entities/arrangements under management by TCSPs and some of the deficiencies identified by the GFSC. The low level of SARs submitted by the sector also raises concerns. The supervisory authorities are working closely with the sector to raise awareness in respect of typologies and red flags associated with the use of legal entities and arrangements and strengthening AML/CFT/CPF controls.

ML Threat and Vulnerability

The threats and vulnerabilities associated with the TCSP sector are broad and there are many different ways perpetrators can use legal arrangements/entities to conceal funds. TCSPs are susceptible to various money laundering threats due to their role in assisting clients with the establishment and management of legal entities, as well as providing related services. Money launderers and criminals may exploit the services provided by TCSPs to hide the origins of illicit funds, evade taxes and engage in other financial crime.

There is a particular risk associated with the use of TCSPs by PEPs. The graph below documents the Domestic vs Foreign PEPs currently utilising Gibraltar based TCSP services.

The data retrieved from the TCSP firms highlights that PEPs applying for TCSP services within Gibraltar remains fairly static. This is due to the increased requirements applicable to PEPs and the lack of appetite from regulated entities to service these clients. In 2024, PEPs, family members and close associates accounted for only 1.76% of all TCSP clients which demonstrates that regulated firms take a cautious approach when onboarding or servicing PEP clients.

Layering through Complex Structures: Money launderers have the ability to use TCSPs to create intricate ownership structures involving multiple layers of companies and

jurisdictions. This complexity makes it difficult to trace the source of funds, as they are moved through various legal entities, banks, and accounts. To minimise this risk, all TCSPs, irrespective of the services they provide are required to conduct due diligence on the whole structure until the ultimate beneficial owners are identified. In addition, TCSPs are obliged to carry out ongoing transaction monitoring which is required to be conducted on a risk-based approach.

Beneficial Ownership Concealment: Although criminals can use TCSPs to establish legal entities with hidden beneficial owners, POCA requires the TCSP to identify and verify the ultimate beneficial owners behind a corporate client. In addition, corporates are required to disclose and submit the beneficial ownership information to the Registrar behind each company incorporated in Gibraltar in line with the beneficial ownership regulations, therefore, allowing for increased transparency. Furthermore, bearer shares are not permitted under Gibraltar law decreasing the risk posed further.

Nominee Shareholding Services: Criminals can use nominee shareholding services to attempt to obscure beneficial ownership. As stated above, the provision of nominee shareholding services is a regulated activity and therefore is authorised and supervised by the GFSC. Additionally, the natural beneficial owner will also be documented within the beneficial ownership register.

Misuse of Offshore Accounts: TCSPs in Gibraltar might be targeted by money launderers seeking to take advantage of the lower corporate tax rates than other jurisdictions.

Asset Holding: Money launderers may use TCSPs to acquire assets through legal entities, thereby disguising the source of funds. However, all TCSPs in Gibraltar are required to assess and document the source of funds/wealth used in the transaction to purchase assets. This is verified by the GFSC through its ongoing supervision of the sector.

Trade-Based Money Laundering: Criminals might use TCSPs to create fake trade invoices and transactions, inflating or deflating prices to move money across borders.

The typologies above are the main uses for money launderers to use corporate structures to conceal the origin of illicit funds. Companies that have been in existence for some time but not used for any purposes, may also be particularly attractive for ML as the company structure gives some legitimacy to the time that an operation has been in existence for a longer period and is often targeted for this specific purpose. Names may then be changed as would shareholding structures under the appointed nominees. As part of the GFSC's supervision, it reviews dormant companies and questions the purpose of these.

Gibraltar mitigates the risks associated to these typologies primarily through the requirements in POCA that obliges all relevant financial businesses to understand, identify, verify and document chains of ownership leading all the way back to natural persons who exercise control over the legal entity in any way. Although there are legal provisions allowing TCSPs to rely on an eligible introducer, data held by the GFSC demonstrates that the overwhelming majority of TCSPs do not apply this approach (92%) so they do not rely on the due diligence undertaken by an introducer, rather this is completed directly by the regulated entity. Therefore, any potential risk posed by an intermediary company is significantly reduced to low.

Section 157 of the Companies Act 2014 does not permit the issuance of bearer shares by Gibraltar incorporated companies and data analysed by the GFSC also confirms that TCSPs do not provide services to any non-Gibraltar client company that allows the issuance of bearer shares. This mitigates the risk further.

Ownership structure and control information is held by the TCSP and is available to the supervisory authority, law enforcement agencies and the Gibraltar Financial Intelligence

Unit. The data on ownership is required to be maintained in an accurate and timely manner and be available to authorities without delay.

TF Threat and Vulnerability

The larger terrorist organisations are structured more like large businesses with the use of corporate structures to manage their assets, increasing the TF threat posed to TCSPs. The threat of terrorist financing is a possibility through the use of corporate structures, however, in the case of Gibraltar based TCSPs the sectoral data analysed by the GFSC demonstrates that 80% of the sector's customers reside or are registered in low to medium low risk jurisdictions which mitigates this risk substantially.

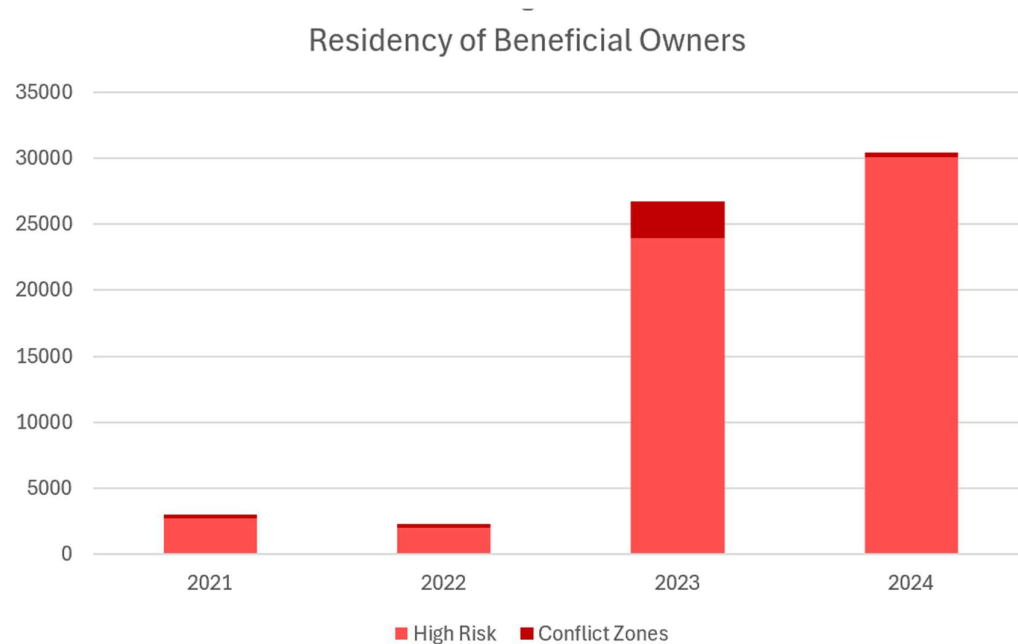


FIGURE 5 – RESIDENCY OF BENEFICIAL OWNERS OF TCSP SECTOR CLIENTS

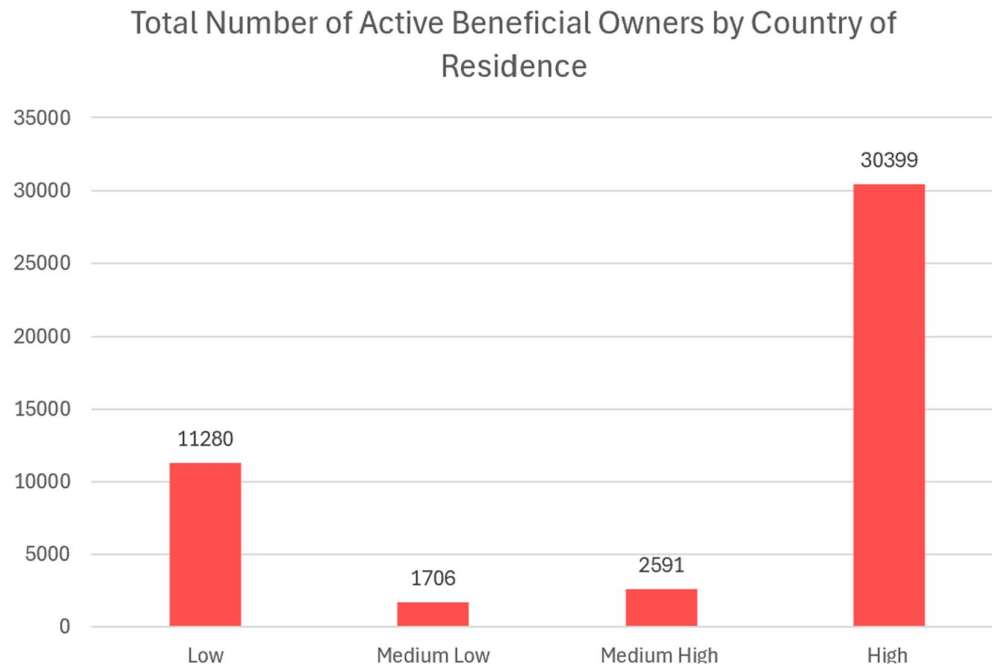


FIGURE 6 – ACTIVITY OF TCSP CLIENTS BY RISK COUNTRY

There has been an increase in the number of customers resident in conflict zones in 2023, this is due to an increase in new conflicts arising globally. Whilst there has been a significant increase, there is no reason to suggest that this is indicative of terrorist financing locally.

Due to Gibraltar's close proximity to Spain, many local entities incorporated within Gibraltar are owned by Spanish residents/nationals. However, this is not indicative of any potential terrorist financing activity as there are no known terrorist organisations operating within the Campo de Gibraltar area in Spain where the majority of these individuals reside. Therefore, these figures are not of concern.

There are several distinctions in the use of corporate structures to facilitate terrorist financing. The main uses are the following:

Use of Shell Companies: Terrorist organisations may use TCSPs to establish shell companies as a front to move funds. These companies might appear legitimate on the surface but are used to funnel money to support terrorism.

Charitable Organisation: TCSPs may be susceptible to the facilitation of terrorist financing through charitable or non-profit organisations that serve as a front for disguising funds to support terrorism.

Regulated entities are required to screen each beneficial owner against several sanctions lists to ensure they are not subjected to local or international sanctions. In addition, the activity risk and country risk must be taken into consideration to ensure that where a client may be operating in a high-risk jurisdiction, it has the appropriate risk mitigation controls in place. Ongoing transaction monitoring and periodic reviews is an important tool for the detection of terrorist financing. All TCSPs are required to continuously monitor all client companies or other types of legal arrangements.

There are no known terrorist organisations operating within Gibraltar, or using Gibraltar based TCSPs as a vehicle to finance terrorism, therefore, the risk is reduced further.

Business Activities of Legal Entities and Legal Arrangements

In assessing the risks of the activities that may be conducted through legal persons and arrangements, there are several types of way perpetrators can use corporate structures in an attempt to hide or conceal the origin of funds.

Front companies used for fraud via false invoicing: Perpetrators may use front companies to apply false invoices to imported items, with the overpayments siphoned off in an attempt to launder or finance terrorism.

Trade-based money laundering: Perpetrators use trade-based money laundering (TBML) to justify the movement of criminal proceeds through banking channels (via letters of credit, invoices, etc.) or through the use of global transactions, often using false documents for 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 with each other to create an information trail to justify transfers of funds of illegal origin. Perpetrators use fictitious loans to justify the movement of criminal proceeds through banking channels — without any economic backing.

Tax Evasion and Avoidance: Some individuals and corporations might use legal arrangements to evade or avoid taxes by shifting assets to jurisdictions with favourable tax regimes or utilizing complex cross-border transactions.

Fraud and Misrepresentation: Legal arrangements can be misused to engage in fraudulent activities, such as falsifying documents or misrepresenting ownership.

Conflict of Interest: In cases where individuals with control over legal arrangements have conflicting interests, they might exploit these structures to serve their personal interests at the expense of others involved.

Regulatory: Some entities may establish legal arrangements to take advantage of regulatory differences between jurisdictions, potentially engaging in activities that are illegal in their home jurisdiction.

Asset Protection: Legal arrangements might be used to shield assets from creditors or to defraud creditors by transferring assets to evade liabilities.

Special Purpose Vehicles (SPVs): These are legal entities created for a specific and narrow purpose, typically distinct from the primary business activities of the companies or individuals involved. These entities are often designed to isolate risks and separate certain assets, liabilities, and financial activities from the parent company or individuals. These may be used to hide assets or liabilities from the parent company or other companies.

Regulated entities such as TCSPs, Banks and Accountants, are required to understand and document the business operations conducted by legal entities/arrangements. Additionally, regulated entities are required to implement a well-defined risk methodology to assign risk scores to the nature of these activities. In recent times, there has been a substantial uptick in the use of legal entities for online trading, which introduces an elevated level of risk due to the global reach of such commerce. In addition to assessing risks related to activities, regulated entities are also required to factor in risks associated with specific countries.

Considerations within the risk assessment should include aspects like the domicile of beneficial owners, the country of origin for funds utilised within the structure and the jurisdiction generating any revenue. Ongoing monitoring plays a significant part to ensure the original purpose behind establishing the legal entity remains consistent over the course of the business relationship. As part of this, identification and reporting of any suspicious activity to relevant authorities are key elements of this process.

ML Threats and Vulnerabilities

Gibraltar companies, or other legal entities managed by a TCSP, may be used at any time for the provision of any of the above purposes, however, there has been minimal cases to date within the jurisdiction to suggest that this is a material risk.

In addition, the significant majority of Gibraltar companies (66%) are established for asset holding purposes with less than a quarter being established for trading purposes.

Nevertheless, these risks are mitigated through the obligations placed on TCSPs under POCA. The regime in Gibraltar treats TCSPs in the same manner as Financial Institutions.

Particularly relevant to mitigating these risks is the ongoing monitoring requirement. TCSPs are required to scrutinise transactions undertaken throughout the relationship to ensure that the transactions are consistent with the firm's knowledge of the customer, its business and risk profile, including where necessary the source of funds and wealth and maintaining up-to-date the documents, or information obtained for due diligence purposes.

In addition, and further enabling a TCSP to scrutinise transactions, Regulation 47 of the Financial Services (Fiduciary Services) Regulations 2020 provides that TCSPs must keep accurate records of transactions entered into, either on its own behalf or on behalf of companies for which directors are provided or trusts or foundations administered. The GFSC's AML/CFT/CPF Guidance Notes further provide that firms, such as TCSPs, must pay special attention to any activity they regard as more susceptible, by its nature, to be related to money laundering or terrorist financing threats related to business activities of legal entities.

The GFSC's enhanced supervisory approach for AML/CFT/CPF purposes, assesses the ML/TF/PF risks, which includes extensive use of on-site and off-site inspections where a regulated entity's compliance with these requirements is assessed. This is a significant contributing factor to the mitigation of risks posed.

The number of companies under management by TCSPs within Gibraltar has been declining for a number of years. TCSPs are attracting and retaining higher value/lower volume business. This category of client typically facilitates a TCSP's ability to undertake more effective ongoing transaction monitoring due to the type and availability of relevant documents decreasing the potential ML risk.

TF Threats and Vulnerabilities:

The assessment of the terrorist financing threat related to business activities of legal entities or legal arrangements shows that terrorists groups do not particularly favour this kind of method to finance terrorist activities as it requires the creation of an opaque structure (illicit legal entity or legal arrangement) or infiltrating the ownership of a legitimate legal entity or legal arrangement. It requires expertise and the ability to plan. Due to the different steps to be taken, it is unlikely that 'clean' money can be collected quickly from this method. Although larger terrorist organisations are structured more like large businesses with the use of corporate structures to manage their assets increasing the TF threat posed to TCSPs, it has not been identified that criminals have used local TCSPs as a method of funding terrorist activities or organisations.

Sectoral data analysed by the GFSC indicates that some TCSPs have clients who are either nationals or resident in higher risk countries or transact business in these countries. The exposure is, however, negligible. Data provided by the TCSP sector demonstrates that only 0.6% of clients serviced by Gibraltar based TCSPs, reside in conflict zone jurisdictions. In addition, Gibraltar has adopted the UK and EU restrictions on providing legal arrangement services to Russian nationals.

Transaction monitoring obligations placed on TCSPs mitigates this threat substantially as the TCSP is obliged to scrutinise transactions. In the instances where the TCSP does not control the client bank accounts, it is required to obtain evidence from the client in respect of transactional information as part of its legal and regulatory obligations.

With regard to legal arrangements such as trusts, there is no evidence to suggest that terrorist organisations are using Gibraltar based TCSPs, there are no known terrorist organisations operating from or within Gibraltar. Additionally, there is reason to suggest that terrorists would not use a trust as a means of funding terrorism on the basis that these types of legal arrangements do not exist in many jurisdictions.

Termination of Legal Entities and Legal Arrangements

The termination of a legal entity or arrangement looks at 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 but now without financial difficulties. Perpetrators may cash out funds from the front company before the illegal activities are detected or before assets are seized by competent authorities, masking the audit trail of money laundered through the liquidated company.

The assessment of the ML and TF threat posed by the termination of a legal entity or arrangement shows that bankruptcy is part of a more global process and some judicial administrators have reported cases where false bankruptcy has been used to launder proceeds of crime.

No cases have been identified in Gibraltar to suggest that this is a method used by criminals locally. This indicates that criminals and criminal organisations perceive this method as unattractive or difficult to access as it requires some logistical and planning capabilities, therefore, reducing the likelihood of this risk.

Gibraltar's regulatory and supervisory regime for Insolvency Practitioners (who would be involved in the bankruptcy process) places the same level of AML/CFT/CPF requirements on them as outlined above for TCSPs. Insolvency Practitioners are also subject to the authorisation and supervisory assessments by the GFSC, including on-site and off-site inspections where client file reviews are undertaken and compliance with all requirements verified. This contributes to the mitigation of risks in this area.

Threat and Vulnerability Assessment

As a finance centre, Gibraltar could be a likely target for money launderers or terrorist financiers looking to exploit weaknesses in the legal or regulatory framework and therefore the threat is probably higher than in other jurisdictions. However, the vulnerability is mitigated because of the legal and regulatory frameworks in place and understanding of the risks by the regulated sector.

The predicate offences indicated by SARs show a prevalence of fraud and tax crimes as the main reasons for the submission of a SAR which is commensurate with the activities that this sector is likely to be misused for.

Legal Persons & Arrangements

Gibraltar has a significantly large TCSP sector. Consequently, this sector may be exposed to the criminal exploitation of otherwise legitimate economic activities and structures. High-end money laundering cases often involve sophisticated schemes and corporate structures designed to conceal the true source of funds and the identity of beneficial owners. As such, corporate structures and trusts can sometimes be used for these illicit purposes due to their ability to provide anonymity, flexibility and a layer of complexity that makes it challenging for authorities to trace the illicit funds back to their origin.

Types of Legal Persons

In accordance with Companies House data, the majority of companies in Gibraltar are managed via a locally regulated TCSP and these play a key role as the gatekeepers for the financial services sector in Gibraltar. During the incorporation process with Companies House, a company is required to provide a range of details such as the registered office address and information on its directors and shareholders. This reduces the risk of corporate structures and trusts from concealing beneficial ownership information and, thereafter, money laundering as well as facilitating other illicit activities.

Type of Legal Entity	Number of live registrations
Private Company	14,087
Private Company limited by guarantee with or without share capital	399
Foreign Company Branches carrying on business in Gibraltar	189
Public Company	22
Limited Liability Partnership	19
European Economic Interest Grouping	4
Public Company limited by guarantee with or without share capital	0

TABLE 20 - NO OF LEGAL ENTITIES AS AT 31ST DECEMBER 2024

There are a number of different legal entity types that can be formed under Gibraltar law. These have been set out in detail below.

Private Company

Private companies form the largest number of legal entities incorporated in Gibraltar. A private company is a firm held under private ownership which, by its articles of association, restricts the right to transfer shares and prohibits any invitation to the public to subscribe for its shares or debentures. There are variety of different types of private companies all of which have different rules for shareholders, members, and taxation.

These private companies are fully distinct legal entities which are either limited by shares or guarantees. There is no restriction on the maximum number of shareholders that Gibraltar registered private companies may have.

The large number of live registrations for private companies is mostly due to its quick formation. The time taken to incorporate a company in Gibraltar is typically three working days. It is an attractive form of legal entity due to the liabilities of the company not being associated with its shareholders. The company is liable for its debts to the full extent of its assets, these liabilities do not extend to the personal assets of its shareholders, unless banks and landlords, for example, seek personal guarantees from the directors, making them personally liable for obligations should the business fail. A private company is also ideal for expansion, this is because it has a perpetual existence so the ownership can pass at any time through the transfer of shares. The fact that private companies are the most commonly used legal entities in Gibraltar, slightly increases the jurisdiction's exposure to money laundering and terrorist financing, in comparison with the other legal entities which are not as widely utilised.

All companies must comply with the provisions of the Companies Act 2014 and there are normally fees for the management of a company. Accounts and other returns are necessary and are by and large, an annual requirement. There are numerous regulations which govern

the administration of a company, with the duties, responsibilities and liabilities of directors being set out in the Companies Act 2014. Due to the requirements placed on private companies under the Companies Act 2014 and that the TCSP sector is robustly regulated in Gibraltar, this mitigates the risks associated with setting up a private company for the purposes of laundering money or financing terrorism to an extent.

Private Trust Companies

A Private Trust Company (PTC) is an entity whose sole purpose is to act as trustee in relation to a specific trust or a group of trusts which are connected. As defined by the Private Trust Companies Act 2015, “Connected Trust Business” refers to the administration of a Trust solely for the benefit of the Settlor and/or for those persons categorised as “Designated Individuals” as well as its “Connected Individuals”. Connected Individuals are defined, under the Act, *“as persons who are connected to the Designated Individual by way of family ties, such as by being a spouse/civil partner, or child of the Designated Individual. Designated Individuals are the persons nominated by a Private Trust Company to be the Designated Individual for the purposes of its Connected Trust Business.”*

A PTC is typically formed due to its ability to deliver a number of benefits and to be easily integrated with other family entities such as an existing company or philanthropic organisation. A PTC is formed with a view to consolidate several family trusts under one umbrella, to retain more family control over a trust’s investments or to allow for long-term structural and administrative flexibility, allowing the PTC to become adaptable when there are changing family circumstances and wishes.

Whilst the PTC is not itself subject to any regulatory regime in Gibraltar, it is required to be managed by a Registered Administrator under the Private Trust Companies Act 2015. These Registered Administrators are always a TCSP which is authorised by the GFSC to carry out these management activities. As outlined above, these TCSPs are subject to an enhanced supervisory approach by the GFSC for AML/CFT purposes. This greatly assists in mitigating the risk of PTCs being used to facilitate ML or TF.

The PTC trustee may not be compensated for its services unless it is authorised by the GFSC and must exercise its duties and powers as a trustee in the usual way. The formation of PTCs also reduces the exposure of the regulated TCSP from becoming unable to continue to act in the event of a corporate insolvency.

All PTCs are private companies and therefore, subject to the same registration and filing requirements as all other private companies; this increases a PTC’s transparency and reduces the risk of criminals seeking to operate a PTC for ML or TF purposes.

Private Company Limited by Guarantee (with or without share capital)

A Private Company Limited by Guarantee without share capital means that it has no share capital or shareholders, but rather, has members who act as guarantors of the company’s liabilities. This means that each member undertakes to contribute an amount specified in the Articles of Association in the event of insolvency or of the winding up of the company.

A Private Company Limited by Guarantee with a share capital is typically classified as a ‘hybrid’ company. This designation arises from the company’s dual limitation, encompassing both shares and guarantees. Consequently, this type of company features two distinct categories of members, shareholders, and guarantee members.

This type of structure is commonly embraced by non-profit organisations who seek to establish their own legal status and distinct identity. Companies which are often incorporated this way include charities, clubs, community activities and property management so as to obtain corporate status. It is possible that non-profit organisations, like their for-profit counterparts, face numerous risks relating to ML and TF. While there is

no evidence of non-profit organisations being abused by terrorists and terrorist organisations in Gibraltar, they continue to be misused and exploited by terrorists through a variety of means worldwide. Gibraltar has an effective legislative framework and ongoing regulatory requirements for charity companies, so risks associated with ML and TF are significantly reduced. At a practical level, there is no material difference in the administration, registration, taxation or management in setting up a private company limited by guarantee for non-profit organisation structures for a trust or foundation.

Foreign Company Branches carrying on business in Gibraltar

Branches of foreign companies that operate in Gibraltar are required to be registered with Companies House as a matter of law under Part XII or Part XIV of the Companies Act 2014. The branch must provide various details to Companies House on registration including its constitution, directorship and membership. There are only 189 foreign company branches carrying on business in Gibraltar. These businesses are required to appoint authorised representatives in Gibraltar to receive served process and must provide Companies House with accounts, annual returns, and any alterations on an ongoing basis. Given that there are currently very few live registrations, in addition to the requirements that it must comply with under the Companies Act 2014, the risk of ML or TF posed by foreign company branches in Gibraltar is deemed to be low.

Public Company

A public company is business which, under law, is permitted to sell its shares to the public. Similar to a private limited company, members involved in a public limited company benefit from limited liability. This implies that unless members have personally guaranteed business loans, members are not held responsible for the company's debts.

These companies, must have at least two directors and when formed, can only commence business activities once it has obtained a trading certificate from Companies House. The Secretary of the Public Company also needs to have specific knowledge and experience to discharge the functions of secretary.

Due to the regulatory requirements involved, criminals are assessed to be highly unlikely to set up public limited companies for money laundering, terrorist financing or proliferation financing purposes.

Limited Liability Partnership

Limited Liability Partnerships (LLPs) allow for a partnership structure where each partner's liabilities are limited to the amount of funds they inject into the business. This means that the business partners of a partnership have distributed the financial risk. This type of structure is typically used for professions which operate as a traditional partnership, such as solicitors and accountancy firms. Additionally, any changes in the particulars of an LLP must be filed in Companies House and all LLPs must file yearly accounts. The ML and TF risks that these legal entities pose is significantly reduced on the basis that there are currently only 19 live LLPs with the majority of them are being utilised as solicitor and accountancy firms. These are professions that are under the supervision of its own supervisory authorities and regulatory regimes, who ensure their firms and regulated individuals comply with AML/CFT requirements under the Proceeds of Crime Act 2015.

European Economic Interest Grouping

A European Economic Interest Grouping (EEIG) is a type of legal entity created under the European Community (EC) Council Regulation No. 2137/85. It is designed to facilitate or develop the economic activities of its members by a pooling of its resources, activities, or skills. An EEIG is not an EU company, rather a vehicle allowing companies or individuals of

different Member States to combine and register in any EU country a grouping that has legal personality and can operate across national frontiers. It is formed to carry out particular tasks for its member owners and is quite separate from its owners' businesses.

An EEIG is similar to a partnership in that it is not intended that the grouping would make profits for itself, therefore, any profits would be apportioned among the members and taxed accordingly.

ML Threat and Vulnerability

Money laundering through the use of private companies is considered an increased risk on the basis that this is the most popular vehicle utilised in Gibraltar and thus the most vulnerable. Nevertheless, any ML risk associated with private companies is significantly reduced on the basis that these legal entities are required to register with Companies House and the Ultimate Beneficial Owner Registrar and disclose information on its shareholders and directors. Additionally, approximately 98% of legal entities in Gibraltar are managed via a TCSP. TCSPs are authorised and regulated by the GFSC and go through a robust application process and are subject to an enhanced supervisory approach by the GFSC for AML/CFT purposes. It is also important to note that the majority of the ML risk in Gibraltar has been significantly mitigated through the implementation of stringent measures, including:

- Compulsory disclosure requirements that compel full disclosure of beneficial ownership information under the Beneficial Ownership Register and relevant legislation. This prevents legal entities from concealing the true identities of beneficial owners;
- The requirement to detect and disclose suspicious transactions involving legal entities; and
- The implementation of stringent Customer Due Diligence (CDD) requirements as imposed on regulated entities under POCA. Therefore, any company which is managed by a TCSP, opens a bank account in Gibraltar or has its accounts managed by a local Accountant, for example, will be subject to CDD requirements in line with POCA.

As highlighted in the sections above, the use of legal entities and structures introduces various money laundering risks. There is a potential for these legal entities to be exploited for money laundering due to specific characteristics such as the ease of establishment, level of complexity and the ease of fund movement. Nevertheless, by actively addressing this risk through a combination of the points detailed above, Gibraltar reduces the potential occurrence of money laundering activities associated with legal entities and structures.

TF Threat and Vulnerability

There are terrorist organisations which continuously adapt their strategies to exploit vulnerabilities within financial systems. One area of concern is the potential use of legal entities for terrorist financing.

Some of the threats Gibraltar faces as a jurisdiction are cross-border transactions, the layering of complex transactions involving legal entities to create a convoluted financial trail and the attempt to conceal beneficial ownership. The terrorist financing risks in Gibraltar, specifically through the use of private companies is considered significantly low on the basis that there are presently no terrorist organisations or groups identified to be operating from or within Gibraltar. Comparable to the strategies employed to counter money laundering detailed above, Gibraltar employs the same mitigation measures to address the risks associated with terrorist financing. In Gibraltar, there is comprehensive transparency, strict due diligence requirements and risk-based strategies which effectively mitigate the risks associated with terrorist financing involving legal entities.

Types of Legal Arrangements

The main types of legal arrangements recognised under Gibraltar law are trusts and foundations.

Trusts

A trust is a legal arrangement where one party, known as the "settlor," transfers assets to another party, called the "trustee," to manage for the benefit of a third party, known as the "beneficiary." Putting it in slightly more detail, the following persons are the key participants in a trust arrangement:

- a. **Settlor:** This is the person who creates the trust and transfers assets into it. They set the terms and conditions of how the trust should be managed and for whose benefit;
- b. **Trustee:** The trustee is the individual or entity responsible for managing the trust's assets. They must act in the best interest of the beneficiaries and follow the settlor's instructions. Trustees have a fiduciary duty, meaning they must act with a high standard of care and loyalty;
- c. **Beneficiary:** Beneficiaries are the individuals or entities who will receive the benefits from the trust. They can be named specifically or identified by a class (e.g., "my children").
- d. **Protector:** The protector is the individual or entity appointed to oversee and safeguard the activities of the trustee. The role of the protector is to ensure that the trustee manages the trust in accordance with the terms of the trust deed and in the best interests of the beneficiaries.

How Does a Trust Work?

At a basic level, a trust works as follows:

- a. **Creation:** The settlor creates the trust by drafting a legal document (usually through lawyers) called a trust deed. This document outlines the trust's terms, including who the beneficiaries are, how the assets should be managed, and any specific instructions for the trustee;
- b. **Funding:** The settlor transfers assets into the trust. These assets can include money, property, investments, or other valuable items.
- c. **Management:** The trustee manages the trust according to the trust deed. This includes making decisions about investing the assets, distributing income or principal to beneficiaries, and handling any administrative tasks;
- d. **Distribution:** The trustee distributes the trust's assets or income to the beneficiaries according to the settlor's instructions. This can happen at specific times, under certain conditions, or when the trust terminates.

Purpose of legal arrangements

There are numerous reasons why someone would establish a trust (or foundation), but by and large they tend to fall within the following categories:

- a. **Asset protection:** Legal arrangements are often established to preserve assets from external risk, such as:
 - the death of a settlor;
 - wasteful actions of the beneficiary;
 - divorce actions;

- claims by creditors or risk of bankruptcy;
 - forced heirship provisions; or
 - concerns about political uncertainty.
- b. **Asset management:** legal arrangements are sometimes entered into for asset management purposes, particularly where:
- there is concern about the beneficiary's capacity, understanding and responsibility to own the assets outright (e.g. the person is a minor);
 - the beneficiary suffers from a mental incapacity or severe disability that prevents them from managing their affairs;
 - the beneficiary is considered impressionable;
 - regulation prevents the beneficiary from owning the asset; or
 - independent oversight of assets is required.
- c. **Business continuity:** Business continuity is also a common reason to establish a legal arrangement, particularly to:
- to separate the management of the business from the enjoyment of the underlying proceeds and prevent fragmentation or dilution of ownership;
 - to ensure that the assets are not prone to short-term views and to reduce the potential disruptions that might otherwise stem from individual ownership, helping to ensure stability for all beneficiaries. With ownership being held on trust, those beneficiaries who are less directly involved in the day-to-day activities may be given a share in the value of the business, and may benefit from an income stream, without acquiring the voting control that comes with outright ownership.
- d. **Privacy:** Trusts provide a layer of privacy. This may be considered important for cases such as the security and safety of high-profile individuals or managing expectations of potential beneficiaries.
- e. **Tax optimisation:** trustees may be exempt from income and other types of tax or taxed at a lower rate compared to companies or the country in which the beneficiaries would be subject to taxation. Identifying the trustees in a jurisdiction where the trustees are tax-exempt avoids the potential for double taxation or a lack of proper reliefs between the countries. This, and the ability to make appointments to beneficiaries at the time of the trustees' choosing, can delay the time when taxation arises on a beneficiary.
- f. **Estate planning and probate:** Trusts may be useful in the context of estate planning as they provide for the administration of interests in property that are contingent and/or subject to shifting, as well as the ability to create and protect future interests in property for people who are not presently ascertainable. Trusts may also play a role in by-passing probate formalities that would otherwise arise on the death of a testator who owns the assets personally. As the legal title to the trust assets is held by the trustee, there is continuity of ownership which is unaffected by the death of the settlor (or a beneficiary). This may avoid practical issues such as where a bank account would otherwise be "frozen" pending the grant of probate; or where assets are owned in different countries.
- g. **Investment or commercial holding vehicle:** Trusts may be used as a holding vehicle for joint investments, such as unit trust type arrangements and pension funds. Trusts may be necessary for conducting certain commercial operations, such as to:

- ring-fence funds to ensure consumer protection (e.g. landlords holding tenants' deposits or travel companies holding funds provided for holidays);
- ring-fence funds for employees (e.g. group life policies that provide lump sum death benefits);
- fulfil a future obligation (e.g. the provision of funeral services or building maintenance services; or in relation to the future decommissioning of oil fields); or
- provide security for contracts (e.g. amounts of additional contingent consideration on the sale of shares or assets; or in relation to financial market bond issues).

Types of Trusts

There are several categories, not all of which are mutually exclusive, and some trusts can fall within more than one category: (such as, for example, an inter vivos discretionary trust):

- Revocable Trust:** The settlor retains the right to modify or revoke the trust during its lifetime. It provides flexibility and can be used for estate planning.
- Irrevocable Trust:** Once created, the settlor cannot change or revoke the trust. It provides greater asset protection and tax benefits but less flexibility.
- Inter Vivos Trust (Living Trust):** Created during the settlor's lifetime, it can be either revocable or irrevocable and is often used to manage assets and avoid probate.
- Testamentary Trust:** Established through a will and takes effect after the settlor's death. It is commonly used to manage assets for minors or provide for specific needs.
- Charitable Trust:** Created to benefit a charitable organisation or purpose.
- Discretionary Trust:** In a discretionary trust, the trustee has the authority to decide how the trust's income and capital are distributed among the beneficiaries. The trustee can consider the needs and circumstances of each beneficiary, providing flexibility to address changing situations.
- Fixed Interest Trust:** A fixed interest trust provides specific beneficiaries with a predetermined interest in the trust's income or assets. The terms of the trust dictate exactly how much each beneficiary will receive and when they will receive it, leaving no discretion to the trustee.
- Life Interest Trust:** Also known as an "interest in possession trust," this type gives a beneficiary the right to receive income from the trust assets or use the assets during its lifetime. After the life interest beneficiary passes away, the remaining trust assets are distributed to other beneficiaries, often called remaindermen.
- Non-Charitable Purpose Trust:** A non-charitable purpose trust is established for a specific purpose rather than for the benefit of individual beneficiaries. These trusts are often used for maintaining family graves, caring for pets, or managing specific assets such as a family business. Unlike charitable trusts, they do not need to benefit the public or a charitable cause. Legal requirements and enforceability of such trusts vary by jurisdiction, but they are recognised in some places like Gibraltar. In Gibraltar, purpose trusts are governed by the Purpose Trusts Act (PTA). The PTA provides for the creation and enforcement of trusts whereby the trustees hold property on trust to carry out a specific purpose, which is not of a charitable nature. The trust document must appoint an Enforcer whose duty it is to enforce the purpose or purposes of the trust. Although there may be more than one trustee in appointment, there must always be at least one Gibraltar licensed trust and company service provider in appointment.

Gibraltar trusts

The most common type of trust in Gibraltar is the inter vivos (and to a lesser extent testamentary) discretionary trust.

Trusts and illicit purposes

Because of their flexibility, trusts lend themselves to abuse and can be used for the following illicit purposes:

- a. Trusts can provide an avenue for concealing the true beneficiaries of assets. Complex trusts structures, coupled with varying degrees of beneficiary information disclosure, can make it challenging to identify the ultimate beneficiaries. This opacity can potentially be exploited for money laundering purposes.
- b. Due to a trust's multi-layered nature, it can facilitate the layering of transactions. Funds can be moved through different trust structures, creating confusion and making it difficult for authorities to trace the origin of funds. Sometimes these techniques can be used to obscure the illicit source of wealth.
- c. Furthermore, discretionary trusts grant trustees the authority to make decisions regarding income and capital distributions, beneficiaries and conditions. While these powers are beneficial for legitimate wealth management, they can also be abused for illicit purposes.

Mitigation against illicit purposes

Under Gibraltar law, these risks are mitigated in the following ways:

- a. Trustees of a Gibraltar trust must obtain adequate, accurate and current information on the identity of all trustees, beneficiaries, protectors, settlors and any other person exercising control over the trust (section 61(1) Trustees Act). They must also record and keep this information for at least five years from the date of the termination of the business relationship as well as record the actions that they took in order to obtain it.
- b. Under Regulation 41A of the Register of Ultimate Beneficial Owners, Nominators and Appointors Regulations 2017 (RUBOR), the Registrar of Ultimate Beneficial Owners or the Gibraltar Financial Intelligence Unit can request any of the information which the trustee ought to have pursuant to section 61(1) Trustees Act (see paragraph (a) above).
- c. When engaging the services of any person conducting relevant financial business as defined under the Proceeds of Crime Act 2015 (which includes most activities within finance and financial services) trustees must carry out due diligence on that service provider to ensure that they are, among other things, fit and proper to provide those services. Conversely, when trustees enter into a transaction with those entities, and that transaction is of the type that would trigger customer due diligence measures for that entity, the trustees must provide that entity with the identity of all trustees, beneficiaries, protectors, settlors and any other person exercising control over the trust (section 61B Trustees Act).
- d. Trustees must also maintain accounting records of all transactions, assets and liabilities for a period of 5 years (section 61(3) Trustees Act).
- e. Trusts which generate tax consequences in Gibraltar must be registered with the Registrar of Ultimate Beneficial Owners pursuant to the Register of Ultimate Beneficial Owners, Nominators and Appointors Regulations 2017 (RUBOR). The trustees of these trusts must submit details of all trustees, beneficiaries, protectors, settlors and any

other person exercising control over the trust via other means. This information can then be accessed by competent authorities and financial intelligence units.

- f. Although trusts which do not generate tax consequences are not registrable, it is widely understood that the vast majority of Gibraltar trusts are managed by TCSPs, who are by law required to properly understand any structure they help establish, manage or administer and obtain as well as retain up to date beneficial ownership information of its customer which, in the context of a trust, includes all other trustees, beneficiaries, protectors, settlors and any other person exercising control over the trust. Purpose trusts must have at least one TCSP in appointment as trustee.
- g. In addition, Gibraltar law also imposes strict ongoing transaction monitoring requirements on its TCSPs so that layering and complex transactions can be detected promptly and disclosed to the relevant authorities. Gibraltar's robust regulatory and legislative framework emphasise the requirement for transparency in legal arrangements including strict due diligence requirements, enhanced beneficiary identification and comprehensive procedures.

The above requirements all work towards helping the relevant authorities to identify and prevent the misuse of Gibraltar trusts for illicit purposes.

Foundations

A Gibraltar foundation is a legal entity that combines elements of both trusts and companies, providing a flexible structure for holding and managing assets. Below are some key points regarding Gibraltar foundations:

- a. **Purpose:** Gibraltar foundations can be established for a wide range of purposes, including private wealth management, estate planning, charitable activities, and holding assets like family businesses or intellectual property. They can serve both charitable and non-charitable purposes.
- b. **Founder:** The individual or entity that establishes the foundation is known as the founder. The founder sets out the foundation's purposes, structure, and governance in a document called the foundation charter.
- c. **Council:** The management and administration of the foundation are carried out by a council, similar to a board of directors in a company. The council acts in accordance with the foundation charter and any additional regulations set by the founder.
- d. **Beneficiaries:** A foundation may have beneficiaries who benefit from its assets and activities. The beneficiaries' rights and interests are defined by the foundation charter and any governing regulations. Unlike trusts, Gibraltar foundations can therefore be established to benefit both purposes and beneficiaries.
- e. **Guardian:** The foundation may appoint a guardian to oversee the council's activities and ensure that the foundation's purposes are being fulfilled. The guardian acts as an additional layer of oversight and can be granted various powers by the foundation charter. Where a foundation is established for a purpose or purposes, there must be a guardian in appointment who can enforce those purposes and ensure that the Council is discharging its duties in respect of them.
- f. **Legal Personality:** Unlike trusts, Gibraltar foundations have their own legal personality, meaning they can own assets, enter into contracts, and sue or be sued in their own name. This provides a clear separation between the foundation's assets and the personal assets of the founder and council members.
- g. **Flexibility and Control:** Gibraltar foundations offer significant flexibility in terms of governance and asset management. The founder can retain a degree of control over the

foundation's activities through the charter and regulations, while also benefiting from the legal and tax advantages of a separate legal entity. The retention of control by the Founder can, however, carries an inherent risk in a money laundering or terrorist financing context.

- h. **Perpetuity:** Gibraltar foundations can exist indefinitely, providing a long-term solution for asset management and succession planning. This makes them suitable for preserving family wealth and ensuring continuity across generations.

Creation and Registration of a Gibraltar Foundation

Creating and registering a Gibraltar foundation involves several steps to ensure that the foundation is properly established and complies with local laws and regulations. Here is a brief overview of the process:

- a. **Drafting the Foundation Charter:** The founder drafts the foundation charter, which is the primary governing document of the foundation. The charter outlines the foundation's purposes, the structure of its council, the rights of beneficiaries, and other essential provisions. It must include details such as the foundation's name, its registered address in Gibraltar, and the initial endowment or assets being transferred to the foundation.
- b. **Preparation of Regulations (Optional):** In addition to the foundation charter, the founder may prepare a set of regulations. These regulations provide more detailed rules on the management and administration of the foundation, including the roles and responsibilities of the council, the appointment of guardians, and procedures for decision-making.
- c. **Appointment of Council Members and Guardian:** The founder appoints the initial members of the foundation council. These individuals or entities will be responsible for managing the foundation's assets and ensuring that its purposes are fulfilled. The council acts similarly to a board of directors in a company. As set out above, where a Foundation is established wholly or partly for the fulfilment of a purpose, a Guardian must be appointed to ensure that the Council is held accountable for fulfilling that purpose.
- d. **Engaging a Licensed Corporate Service Provider:** To proceed with the registration, the founder must engage a licensed corporate service provider in Gibraltar or elsewhere. This provider will assist with the necessary paperwork and ensure that all legal requirements are met. A Gibraltar foundation must always have a TCSP on the Council.
- e. **Submission to the Gibraltar Registrar of Foundations:** The foundation charter and any accompanying regulations are submitted to the Gibraltar Registrar of Foundations, along with the prescribed application form and registration fee. The registrar reviews the documents to ensure compliance with the Private Foundations Act 2017.
- f. **Issuance of Certificate of Registration:** Upon approval, the Registrar issues a certificate of registration, officially recognizing the foundation as a legal entity in Gibraltar. The foundation is then entered into the public register of foundations, providing legal certainty and transparency.
- g. **Endowment of Assets:** The founder transfers the initial assets or endowment to the foundation. These assets can include cash, property, shares, or other valuable items. The transfer is carried out according to the terms specified in the foundation charter.
- h. **Ongoing Compliance:** The foundation must comply with ongoing legal requirements, such as filing annual returns, maintaining proper accounting records, and adhering to any other obligations set forth by Gibraltar law. The foundation's council and any

appointed guardian must ensure that these requirements are met to maintain the foundation's good standing.

Foundations and illicit purposes

Because of their flexibility, foundations, like trusts, lend themselves to abuse and can be used for the same illicit purposes set out in paragraph 8 above relating to trusts.

Mitigation against illicit purposes

Under Gibraltar law, these risks are mitigated in the following ways:

- a. The Council of a Gibraltar foundation must obtain information on the identity of all councillors, beneficiaries, guardians and founders and maintain it for at least 5 years (section 25(14) Private Foundations Act 2017).
- b. Under Regulation 41A the Registrar of Ultimate Beneficial Owners or the Gibraltar Financial Intelligence Unit can request any of the information which the foundation council ought to have pursuant to section 25(14) Private Foundations Act 2017 (see paragraph (a) above).
- c. When engaging the services of any person conducting relevant financial business as defined in the Proceeds of Crime Act (which includes most activities within finance and financial services) carry out due diligence on that service provider to ensure that they are, among other things, fit and proper to provide those services. Conversely, when trustees enter into a transaction with those entities, and that transaction is of the type that would trigger customer due diligence measures for that entity, the trustees must provide that entity with the identity of all trustees, beneficiaries, guardians, settlors and any other person exercising control over the trust (section 61B Trustees Act).
- d. Councillors must also maintain accounting records of all transactions, assets and liabilities for a period of 5 years (section 37(1) Private Foundations Act 2017), as well as prepare annual income and expenditure accounts and balance sheets.
- e. Foundations which generate tax consequences in Gibraltar must be registered with the Registrar of Ultimate Beneficial Owners pursuant RUBOR. The Council must submit details of all councillors, beneficiaries, guardians and founders. This information can then be accessed by competent authorities and financial intelligence units.
- f. All Gibraltar foundations must have at least one TCSP in appointment on the Council, who are by law required to properly understand the structure and obtain and retain up to date beneficial ownership information of its customer which, in the context of a foundation, includes all other councillors, beneficiaries, guardians and founders.
- g. Gibraltar law also imposes strict ongoing transaction monitoring requirements on its TCSPs so that layering and complex transactions can be detected promptly and disclosed to the relevant authorities. Gibraltar's robust regulatory and legislative framework emphasise the requirement for transparency in legal arrangements including strict due diligence requirements, enhanced beneficiary identification and comprehensive procedures.

The above requirements all work towards helping the relevant authorities to identify and prevent the misuse of foundations.

Charitable Trusts

Charitable trusts operate similarly to other trust structures, with the exception that they are set up to benefit certain charitable purposes, rather than individual beneficiaries.

Charitable trusts and illicit purposes

While serving critical humanitarian and social roles, charities can also be particularly vulnerable to exploitation for money laundering and terrorist financing. The inherent nature of charitable operations, often involving large and frequent cash flows, international transactions, and the provision of services in high-risk areas, creates numerous opportunities for illicit activities. In particular, charities can be vulnerable for the following reasons:

- a. **High Volume of Cash Transactions:** Charities often receive donations in cash, which can be difficult to trace. Large volumes of cash can be used to disguise the origin of illicit funds and integrate them into the legitimate financial system.
- b. **Complex Financial Transactions:** Charitable organizations frequently engage in complex financial transactions, including cross-border transfers. These activities can obscure the trail of funds, making it challenging to monitor and trace the flow of money.
- c. **Operations in High-Risk Areas:** Many charities operate in regions with weak regulatory environments, conflict zones, or areas with high levels of corruption. These conditions make it easier for criminals and terrorists to exploit charitable funds without detection.
- d. **Lack of Financial Controls:** Smaller charities in particular, may lack robust financial controls and governance structures. Weak internal oversight can lead to mismanagement or diversion of funds for illicit purposes.
- e. **Third-Party Involvement:** Charities often work with third parties, such as local partners, subcontractors, and intermediaries. These relationships can be used to siphon off funds, divert them to unintended purposes, or cover up the true destination of the money.
- f. **Donor Anonymity:** The anonymity of donors, especially in online and cash donations, can be exploited to funnel illicit funds through charitable organizations. This lack of transparency makes it difficult to conduct thorough due diligence on the sources of donations.
- g. **Misuse of Charitable Status:** Criminals and terrorists can establish fake charities or infiltrate legitimate ones to take advantage of the organization's tax-exempt status and positive public image. This misuse can facilitate the laundering of money and the financing of terrorist activities under the guise of legitimate charitable work.

The above vulnerabilities may give rise to the following risks:

- a. **Integration of Illicit Funds:** **Money laundering through charities can involve the integration** of illicit funds into the financial system. Criminals can donate dirty money to a charity, which then uses or invests the funds, thereby legitimizing the proceeds of crime.
- b. **Diversion of Funds:** Terrorist organizations can infiltrate charities or establish their own to divert funds intended for humanitarian purposes to finance terrorist activities. These funds can be used for recruitment, training, logistics, and operations.
- c. **Exploitation of Resources:** Charities often have extensive networks and resources that can be exploited by terrorists for logistical support, including transportation, safe houses, and communication channels.
- d. **Reputation Damage:** The involvement of a charity in money laundering or terrorist financing can severely damage its reputation, leading to loss of public trust and

funding. This can undermine the charity's ability to carry out its legitimate activities and support its beneficiaries.

Mitigation against illicit purposes

The Charities Act provides a robust registration framework for Gibraltar charities. Although where there are particular reasons for doing so, non-trust entities may be registered as charities under the Charities Act, the Charities Commissioner expects charities to be structured under trusts, and the vast majority of them are. As such, the mitigation measures for trusts, set out in paragraph 9 above, apply to charities. In addition, the Charities Act provides for the Commissioner to assist, exchange information and cooperate with domestic authorities (which include not only law enforcement authorities but also regulatory authorities and Government authorities), foreign Commissioners and foreign authorities in relation to any particular investigation or generally. More recently, the Charities Act was amended to include an obligation for the Charities Commissioner to use its best endeavours to reduce the scope for an activity to be carried on by a charity for a purpose connected with financial crime, in particular by:

- a. developing policies to promote accountability, integrity, and public confidence in the administration and management of charities;
- b. encouraging outreach and educational programmes to raise and deepen awareness among charities as well as the donor community about the potential vulnerabilities of charities to financial crime, including terrorist financing abuse and terrorist financing risks, and the measures that charities can take to protect themselves against such abuse;
- c. encouraging charities to develop and refine best practices to address the potential vulnerabilities of charities to financial crime, including terrorist financing risk and vulnerabilities and thus protect them from abuse; and
- d. encouraging charities to conduct transactions via regulated financial channels, wherever feasible, keeping in mind the varying capacities of financial sectors in different areas of urgent charitable and humanitarian concerns.

Asset Holding and Asset Protection Vehicles

An Asset Protection Trust (APT) is a trust vehicle that holds an individual's assets with the purpose of shielding them from creditors, making APTs the strongest protection against creditors, legal proceedings, or judgements against a person's estate. In Gibraltar, APTs are found to be commonly kept within families so this reduces the risk of the APT being used to facilitate ML or TF.

An APT is a self-settled trust in which the settlor can be designated as a permissible beneficiary and thus, permitted to access the funds in the trust account. Provided that the APT is properly structured, its aim is that creditors will not be able to reach the trust's assets due to it having a separate legal personality. The use of APTs may pose a reduced level of ML and TF risks because it creates a layer of legal separation between the individual's personal assets and the assets held within the trust. This separation could make it more challenging for illicit funds to be intermingled with legitimate financial transactions, adding a level of transparency and accountability.

APTs are registerable in Gibraltar. The Trustees must be companies with permanent residential addresses in Gibraltar and must be registered with the GFSC. Even though APTs are not actively regulated by the GFSC, a register of these is maintained by the GFSC therefore, increasing transparency. At present, there are 22 APTs registered with the GFSC so this, combined with the factor detailed above, illustrates that the overall ML/TF risk is deemed as low.

ML Threat and Vulnerability

Gibraltar has a long standing, regulated TCSP sector which requires all professional trustees to be regulated and supervised by the GFSC for compliance with all AML/CFT requirements as relevant financial businesses.

While it is possible to be a trustee of a Gibraltar trust without being authorised (e.g. acting in a personal capacity), it has been identified that the vast majority of trusts in Gibraltar are managed by regulated professional trustees. The main ML risks lie in the ability to disguise funds in a trust structure and then to distribute the trust funds as a legitimate disbursement of the trust. Due to the regulated nature of the activities conducted by the trustees, adequate controls are in place to mitigate the misuse of trust funds by trustees.

Recent onsite assessments by the GFSC have revealed notable improvements within the TCSP sector indicating that there is an enhanced grasp of money laundering and terrorist financing requirements. This includes a heightened awareness of their obligations, essential functions, and regulatory duties.

There remains a potential threat posed by professional enablers who might collaborate with criminals to establish and oversee trusts or foundations for illicit purposes. Nevertheless, Gibraltar has a strong regulatory framework and effective regulatory oversight which ensures transparency as well as the adherence to internationally recognised AML/CFT standards

It is important to note that robust legislative frameworks are implemented to mitigate these risks, supported by stringent measures aimed at detecting and preventing money laundering. Additionally, the substantial regulatory oversight of TCSPs in Gibraltar plays a pivotal role in significantly reducing these potential risks.

Overall, other types of legal arrangements are so inconsequential in use that they do not raise material concerns. Other types of legal arrangements also require the involvement of professional advisors increasing the likelihood of discovery/reporting of suspicion or knowledge of money laundering or terrorist financing so any risks are significantly reduced. It is important to note that the regulatory framework for the TCSP sector in Gibraltar is a significant mitigating factor in that it has been in existence since 1990 and has been subject to AML/CFT obligations and measures for many years. This industry's regulatory framework includes barriers to entry, fitness and propriety checks on ultimate beneficial owners, officers and controllers of the TCSPs as well as on-site and off-site inspections of verification of systems and controls. Additionally, Gibraltar's TCSP industry is small in comparison to its peer jurisdictions and is insignificant in a global context.

TF Threat and Vulnerability

The potential use of legal arrangements as conduits for terrorist financing, specifically trusts and foundations, poses a low risk in Gibraltar. Despite there being no evidence of terrorist organisations or groups having been identified in Gibraltar, the risk of professional enablers becoming involved in collaborations with criminals is inherently present. Although the risk of terrorist financing taking place via a Gibraltar based trust or foundation is generally low, criminals may still attempt to conceal or hide any transactional activities relating to terrorist groups or activities, specifically through the use of nominee shareholders, which allow individuals to remain anonymous or use false identities. There is always a risk of terrorist organisations/groups seeking to use TCSP services to establish front companies that appear legitimate but are, in fact, conduits for transferring funds to support terrorist activities. However, there is no evidence to suggest that legal arrangements are used for these purposes in Gibraltar. The attractiveness of trust structures for TF purposes is considerably less than ML, as this will require collusion on behalf of the regulated trustees. Similar considerations apply for foundations.

There are various requirements in place for legal arrangements to conduct themselves in a proper manner, and all TCSPs are required to have in place a risk-based approach in respect of the countries, nationality and residency involved in any of its business relationships which ensure that when reviewing the movement of funds, these fall in line with the expected activity, reducing any terrorist financing risks significantly. For these reasons, the TF risk has been assessed as low.

7.3 Money Services Businesses (MSBs) and Money Value Transfer Services (MVTs)

Currency Exchange

Currency Exchange enables the conversion of funds between different currencies at a specified rate determined by the service provider.

Currency Exchange is a widely used service in Gibraltar due to the land border it shares with Spain.

Composition and size of the Financial Sector - Entities that provide foreign currency exchange services

Number of firms that provide foreign exchange services registered/licensed domestically	7
Number of firms that have branches and subsidiaries abroad	0
Total number of client service locations	11 (7 institutions and 4 branches)
Total number of currency exchange transactions above the customer due diligence threshold (5,000€)	6,223
Total number of clients	1,476

TABLE 21 - MATERIALITY OF MSB SECTOR AS AT 31 DEC 2024

All currency exchange providers within Gibraltar are regulated entities and are subject to compliance with the legislative and regulatory standards and requirements set by the GFSC. There are currently 9 currency exchange providers operating in Gibraltar.

The money laundering threat associated with currency exchange is the ease with which large sums of money can be converted, providing organised crime groups with an easier path to legitimise illicit funds.

Due to Gibraltar's proximity to Spain, there is a demand for the exchange of currency on a regular basis. There is a regular flow of tourists entering Gibraltar via use of the airport or land border with Spain that requires currency conversion. Gibraltar also has over 10,000 cross-border workers residing in Spain who need to exchange their earnings into Euro. Given that money laundering through currency exchanges does not require any specific planning or expertise, this method can be appealing to criminals.

The table below sets out data gathered through the GFSC's Financial Crime Supervisory

Return relating to the number of SARs relating to the sector from 2021-2024:

Disclosures to GFIU	2021	2022	2023	2024
Money Laundering	1	5	13	7
Terrorist Financing	0	0	0	0
Other Reasons	0	0	0	1

TABLE 22 - SARS RELATING TO THE SECTOR FOR MSB AND MVTs

The low level of SARs relating to this sector can be attributed to the currency exchanges' challenges in reporting suspicious transactions or activity due to incomplete customer identity documentation. This is because customers may leave the firm premises without providing any identifiable information and effectively, ending the transaction. This presents a hurdle in effectively reporting suspicious transactions or activity as the currency exchange is unable to provide any meaningful information to the Gibraltar Financial Intelligence Unit to identify the subject.

Transfer of Funds

Money value transfer services (MVTs), or money remittance, is a payment service defined under the Financial Services Act 2019. It involves receiving funds from a payer, with no need to establish payment accounts in the names of the payer or the payee. This service is solely intended for transferring a corresponding amount to a payee or to another payment service provider acting on behalf of the payee and/or where such funds are received on behalf of, and made available to, the payee. Customer due diligence requirements when effecting transactions via the use of an MVTs provider within Gibraltar is €1,000.

MVTs is a regulated activity in Gibraltar, requiring authorisation by the GFSC, and the relevant providers are subject to the legislative requirements contained within the Proceeds of Crime Act 2015. Gibraltar has two MVTs providers operating within the jurisdiction as agents of global MVTs providers. Both of these MVTs are also regulated Currency Exchanges, subject to ongoing supervision by the GFSC and who have been verified to have appropriate AML/CFT/CPF systems and controls in place.

The entities acting as agents of either of the global MVTs providers are also required to comply with the additional controls set by the provider in question (e.g. the provision of additional ongoing training on the threats related to this sector and raising awareness of suspicious activity reporting), facilitating the reduction of ML and TF risks.

Payment Services

Payment services institutions are authorised and regulated by the GFSC under the Financial Services Act 2019. These entities cover a wide variety of services, including:

- services enabling cash to be placed on a payment account and all of the operations required for operating a payment account;
- Services enabling cash withdrawals from a payment account and all of the operations required for operating a payment account;
- execution of payment transactions, including transfer of funds on a payment account with the user's payment service provider or with another payment service provider;
- execution of payment transactions where the funds are covered by a credit line for a payment service user;
- issuing of payment instruments; and
- acquiring of payment transactions.

A 'payment transaction' is generally defined as an action initiated by the payer, on their behalf, or by the payee, involving the placement, transfer or withdrawal of funds, irrespective of any underlying obligations between the payer and the payee.

Perpetrators may use this method to channel their funds through bank accounts and the financial system. This may involve wire credit and transfers, debit transfers, (peer-to-peer) mobile payments and internet-based payment services.

There are currently no payment services institutions in Gibraltar, meaning the risk is mitigated in practice.

ML Threat and Vulnerability Assessment

The money laundering threat associated with currency exchange is the ease with which large sums of money can be converted, providing organised crime groups with an easier path to legitimise illicit funds.

Gibraltar's authorisation and regulatory framework provides significant mitigation against the risk of money laundering. The GFSC is responsible for the oversight and supervision of currency exchanges and as part of this, a thematic review was conducted to understand the overall AML/CFT risks applicable to the industry. The review outlined that the currency exchanges operating within Gibraltar have a good understanding of the relevant risks and appropriate systems of control. The shortcomings identified for some firms have now been remediated to a satisfactory level. Therefore, this reduces the overall ML risk posed within the jurisdiction.

Additionally, through its supervisory programme, the GFSC has established that most currency exchanges do not accept high-value notes unless they can be satisfied of their source and origin which also reduces the level of ML risk posed.

The majority of transactions carried out within Gibraltar relate to tourists exchanging small denominations, cross-border workers exchanging salaries and established businesses converting funds. To enhance transparency and reduce ML risk, the GFSC has imposed a lower threshold above which due diligence must be applied for one-off transactions (€5,000) than what is mandated by international standards.

Regulated entities are required to submit returns to the GFSC indicating the number and value of transactions, including those below €5,000, the sourcing of currency and destination of the transaction. This ensures an appropriate level of control and monitoring over the business carried out by the exchanges which reduces the ML risk further.

MVTS, in many instances, rely on cash allowing for speedy transactions. Due to their specific features and in particular their reliance on agents, MVTS can be provided in high risk countries and may be used by high risk customers. Transactions via MVTS providers are subject to specific monitoring and checks. Therefore, the most prevalent risks in the MVTS sector are the cash intensive nature of the service, the high speed and volume of transfers and transfers to high risk jurisdictions.

Organised crime groups tend to use this method in manipulating the agents who provide this service to help facilitate the flow of funds. There are no known organised crime groups operating in Gibraltar and therefore, there is no evidence to demonstrate that MVTS providers are being exploited for ML purposes.

The assessment of the ML threat associated with payment services concerns both the depositing and withdrawing of funds (i.e. deposits on account and use of this account). This method may be frequently used by criminals, with the funds being from non-legitimate origins. However, it requires some planning and knowledge of how banking systems work which may be less appealing to the perpetrator.

The inherent risk exposure is high due to the nature of payment services, as they involve very significant volumes of products and services. Although payments are typically traceable to identified accounts due to the payment services requirements, they may still involve interactions with higher risk customers or countries, including cross border movements of funds. They also interact with new payment methods (mobile/internet), which may increase the level of risk exposure because they imply a non-face-to-face business relationship.

Gibraltar recognises payment services institutions as a relevant financial business under POCA, therefore they are subject to all AML/CFT obligations, as well as the authorisation and supervisory regimes of the GFSC. As there are no payment services institutions in Gibraltar, the impact and vulnerability of a potential ML risk is significantly reduced.

TF Threat and Vulnerability Assessment

The main risk associated with TF concerns the high volume of cash transactions that currency exchanges typically handle, making it difficult to trace the origin and destination of funds effectively. This creates a potential avenue for terrorist organisations to exploit these businesses for terrorist financing purposes. Additionally, Gibraltar's proximity to Spain and its land border makes it susceptible to terrorist actors seeking to move illicit funds across international borders. To mitigate these risks, the GFSC has implemented a wide range of regulatory and reporting requirements and follows an enhanced AML/CFT/CPF supervisory approach for each regulated entity.

The threat associated with MVTs providers is that it does not require any expertise to use the services making it particularly appealing to terrorist groups. MVTs providers facilitate the transfer of cash to destinations worldwide, including high risk jurisdictions and conflict zones, without an account being required.

Terrorist groups use this method as it also allows for the movement of small denominations from various global locations, aiding in obscuring the true source of funds used for funding attacks.

The largest proportion of transactions undertaken by the MVTs providers in Gibraltar are to jurisdictions of which Gibraltar has large migrant communities, justifying these transactions. The sectoral data analysed by the GFSC through its Annual Financial Crime Supervisory Return has demonstrated that Gibraltar's exposure to high risk countries and conflict zones through the use of MVTs providers is low.

There are no known terrorist groups or organisations in Gibraltar, which decreases the overall TF risk posed. There is also no evidence to suggest that local MVTs providers are being exploited for illicit purposes.

The assessment of TF threats linked to payment services shows that account-based transactions can be used by terrorists to store and transfer funds and used to pay for the services or products needed to carry out their operations, in particular, when processed through the internet. The majority of terrorist cells have usually derived some income from legal sources — usually received through the formal banking system — and use bank accounts and credit cards both for their everyday economic activities and for attack-related expenses. Due to the account-based elements, terrorist groups' tendency to rely on this risk scenario is more limited, however, their capability to use it is quite high.

Payment services allow cross-border transactions that may rely on different mechanisms of identification that may lead terrorists to use a false identity. Consequently, law enforcement agencies and authorities often struggle to trace the source or recipient of the transaction. In Gibraltar, payment services are subject to POCA requirements, which do not allow for any anonymity. While the use of payment services requires specific skills, these skills are relatively common within terrorist groups and do not constitute an obstacle (e.g. mobile/internet payments are quite easy). As there are no payment services institutions locally, this reduces the risk exposure.

The threat of risk exposure is typically higher due to the characteristics of payment services, as they involve very significant volumes of products and services. Although payments are generally traceable to identified accounts, they may interact with very significant volumes of higher risk customers or countries, including cross border movements of funds. They also

interact with new payment methods, which may increase the level of risk exposure because they imply a non-face-to-face business relationship.

Gibraltar recognises payment services institutions as a relevant financial business under POCA and therefore they are subject to all the AML/CFT/CPF obligations in line with the GFSC's authorisation and supervisory regimes. As there are no payment services institutions in the jurisdiction, the impact and vulnerability of a potential TF risk is minimal.

7.4 Securities Sector

The securities sector plays a key role in the global economy. The products and services provided by this sector act as a potential means through which individuals and entities can access the financial system on a potentially larger scale. Excluding the credit institutions authorised for the provision of investment-related services, Gibraltar's securities sector is comprised of:

- 9 investment managers; and
- 5 investment dealers (1 of which is an incoming branch passporting services from the United Kingdom on a freedom of establishment basis).

The securities sector is subject to supervision by the GFSC. Throughout 2023, the GFSC has carried out an AML/CFT/CPF thematic review of all investment managers & dealers, publishing the cross-sectoral findings identified by way of its onsite inspections within its Investment Firm Sector Thematic Review Report. As a whole, the GFSC identified various areas for improvement across the sector and continues to work closely with each entity to ensure that any deficiencies are appropriately addressed.

Composition and size of the Financial Sector - Investment/Securities Industry	
Number of Investment Firms:	12
Number of clients	4840
Assets under management	£2,093,515,877

TABLE 23 - MATERIALITY OF SECURITIES AND FUNDS SECTOR AS AT 31 DECEMBER 2024

Since 2019, the overall activity of the securities sector has decreased significantly, primarily as a result of the United Kingdom's exit from the European Union. This can be observed in significant decline in transactional activity facilitated by the securities sector, as set out within the graph below. This is mirrored in part by the overall decrease in the number of SARs disclosed by the sector to the GFIU from 2018 to 2024. The low volume of reported SARs, however, also corroborates the observed general need for strengthened AML/CFT/CPF controls.

Broker-Dealers

Broker-dealers play a crucial role in the stability of financial markets by both providing liquidity and facilitating trading activity. Broker-dealers will either act as intermediaries facilitating transactions between buyers and sellers or engage in the purchase and sale of securities on their own account.

Broker-dealers are susceptible to abuse by criminals primarily on the basis that they allow the movement and handling of large sums of funds pertaining to a wide variety of financial instruments. It is typically considered that broker-dealers involved in international trading activities, are exposed to higher levels of ML & TF risk. This is due to the swift and appealing nature of cross-border investment transactions in allowing the movement of funds between jurisdictions and obscuring their potential illicit origin. In the case of Gibraltar investment firms, however, the United Kingdom represents the singular jurisdiction with the highest

proportion of transactional exposure (whereas exposure to high risk jurisdictions makes up >1%). This is therefore considered to decrease the level of vulnerability in the sector.

Multilateral Trading Facilities (MTFs) & Organised Trading Facilities (OTFs)

Multilateral & organised trading facilities serve as venues for the buying, selling and trading of a wide array of financial instruments. While MTFs primarily focus on the purchase and sale of equity and equity-related instruments, OTFs are able to facilitate the trading of a wider array of assets. In Gibraltar there are no MTFs or OTFs.

When engaging in trading activity via an MTF or OTF, criminals may employ market manipulation techniques to inflate or deflate the price of a listed instrument as a means to generate profits that legitimise the origin of illicit funds. Rapid and complex trading strategies may also serve as a means to obscure illicit activity. The type of financial instrument associated with a transaction can potentially introduce additional layers of complexity (such as in the case of derivatives and other complex instruments). This, however, is mitigated in practice on the basis that Gibraltar currently has no authorised MTFs.

The use of an MTF or OTF is not typically considered a common or attractive means through which terrorist actors gain access to the financial system. This is in part as a result of the transparency associated with MTF & OTF market venues, as well as the typical use of small amounts of funding for terrorist financing purposes in comparison to the typically larger volumes traded on such venues. This is further mitigated by the fact that there are no existing MTFs/OTFs locally.

Portfolio Managers & Investment Advisors

Portfolio managers are tasked with considering the investment decisions associated with a portfolio of assets on behalf of their clients. Investment advisors provide clients with advice on the management and diversification of their investment portfolio. The primary goal of both services is to aid in achieving the financial objectives of an entity/individual in a manner that is in-keeping with their risk tolerance. Of the 13 investment firms established in Gibraltar, there is a total of:

- 6 firms authorised for the provision of portfolio management services; and
- 12 firms authorised for the provision of investment advice.

When engaging in investment advisory or management services, criminals are known to misclassify the source of their income or revenue as a means to provide false explanations for their deposit and withdrawal behaviour. They are also known to engage with advisors and managers in a wide array of jurisdictions in order to ensure that no singular party has full oversight of the extent of their earnings. As stated above, however, there has been an overall significant decrease in the activity of Gibraltar's securities sector and the value of funds managed by (or advised on) by the sector has decreased as a result. This lowers the level of risk associated with the provision of these services in or from Gibraltar.

ML Threat & Vulnerability Assessment

The features of the securities sector may present a potentially attractive means through which criminal actors may integrate illicit funds into the financial system. This is predominantly as a result of the speed at which transactions can be executed, the potential cross-border nature of transactional activity and the complexity with which financial instruments can be traded.

The ultimate vulnerability faced by this sector in Gibraltar is mitigated by the GFSC's supervision. The low volume of SARs reported to the GFIU, together with the general observations of the GFSC's investment firm thematic review, however, indicate that the controls of the sector may not be commensurate with the level of risk posed. Following on from the Thematic Review, the GFSC is actively working with the sector to enhance standards and controls in respect of its AML/CFT/CPF compliance.

TF Threat & Vulnerability Assessment

The activities of the securities sector are typically associated with the large scale use/movement of funds. Abuse of the sector for the purposes of gaining or moving the limited funding typically associated with terrorist organisations is therefore not considered a common occurrence. This is mitigated further by the high level of prerequisite knowledge typically required to manipulate and abuse financial markets for these purposes.

From 2021 to 2024 no SARs relating to terrorist financing have been reported by the sector to the GFIU. The exposure to high risk jurisdictions faced by the sector is also minimal, representing >1% of all transactional activity and approximately 2% by customer residence. The level of TF risk posed by the sector is therefore considered to be low.

7.5 Funds Sector

Funds serve as investment vehicles allowing individuals and corporates to indirectly invest in equities and other assets. Investors purchase units in a fund and a fund manager then combines and oversees the pooled money in accordance with the fund's specified rules and objectives.

For collective investment schemes, the GFSC mandates the publication of a prospectus and other key documentation that outlines the management guidelines. Additionally, a fund administrator is mandated by law to be appointed to oversee the fund's AML/CFT/CPF processes such as the onboarding, ongoing monitoring, subscriptions, and redemptions of its investors.

There has been a rise in the number of cryptocurrency funds established in Gibraltar. The jurisdiction has a total of 11 cryptocurrency funds which are all Experienced Investor Funds registered with the GFSC. Cryptocurrency funds are investment funds that primarily focus on cryptocurrencies and related assets. These funds allow investors to gain exposure to the cryptocurrency market without the investors directly holding the virtual assets themselves. Cryptocurrency funds operate similarly to traditional investment funds, where a pool of capital is held in a joint vehicle managed by a professional fund manager. Although cryptocurrency funds may present a higher risk than traditional fiat funds, this is somewhat mitigated as 100% of these are currently authorised as Experienced Investor Funds and therefore have a dual layer of reporting requirements by both the fund and fund administrator.

		No. Transactions Received	No. Transactions Issued	Value of Funds Received (£)	Value of Funds Issued (£)
Conflict Zone	China, People's Republic of	0	0	0	£0
	Lebanon	0	9	£17,834	£0
	Nigeria	0	0	0	£0
	Türkiye	0	2	£103,877	£0
	Ukraine	0	0	£0	£0
Produces & or transit drugs	El Salvador	0	0	£0	£0
	Guatemala	10	85	£86,910	£1,786

TABLE 24 - TRANSACTIONS BETWEEN THE SECURITIES SECTOR AND HIGH RISK JURISDICTIONS IN 2024

Throughout 2021 and 2022, the GFSC carried out a Thematic Review of the sector to gain a better understanding of the risks, threats and vulnerabilities pertaining to the funds industry in relation to money laundering, terrorist financing, and proliferation financing. The Thematic Review covered an assessment of all AML, CFT and CPF legislative and regulatory requirements. Onsite visits were carried out on all Experienced Investor Funds (EIFs), Alternative Investment Fund Managers (AIFMs), and Collective Investment Scheme administrators (CISAs) which form part of the local Funds industry.

The funds sector is unique as it typically incorporates a second line of defence, often in the form of a CISA. CISAs are generally regulated within the jurisdiction in which they operate and are required to be authorised in Gibraltar. This provides an additional layer of oversight and regulation.

The funds sector could be used by perpetrators to clean illicit funds, however, there are various layers of oversight when investing in fund products which mitigates the potential risks associated with the funds sector to some degree.

Private Funds

Private funds are designed for the promoter's friends and family and, in some cases, family office structures who do not seek to onboard external investors. The Financial Services Act 2019 imposes certain restrictions on Private funds, which are primarily intended to be aimed at specific categories of individuals and limited to a maximum of fifty subscribers.

Private funds are subject to the Financial Services (Alternative Investment Fund Managers) Regulations 2020 and are obliged to register as "small self-managed AIFMs" with the GFSC. Currently, there are 123 small self-registered AIFMs registered with the GFSC, however, approximately 40% of these are also authorised by the GFSC as EIFs so these are fully regulated mitigating potential risks further.

Private funds can take the form of partnerships, unit trusts or companies. Among those registered with the GFSC, most are companies, with a few exceptions being partnerships and limited partnerships. The legal framework dictates that companies and partnerships registered within Gibraltar must have a registered office within the jurisdiction. As a result, private funds typically appoint a Trust and Company Service Provider (TCSP) to provide registered office services, company management and professional trusteeship services. TCSPs are subject to a robust supervisory regime by the GFSC for AML/CFT/CPF purposes and are considered a relevant financial business under the Proceeds of Crime Act 2015. Therefore, TCSPs are required to comply with all AML/CFT/CPF requirements and must conduct appropriate customer due diligence on the private funds and their investors. This increases transparency and helps mitigate the risk of private funds being a conduit for ML, TF and PF.

The establishment of a private fund requires expertise in establishing the appropriate legal structure (e.g., companies, trusts, partnerships) and structuring the fund itself. This complexity acts as a deterrent against potential misuse for ML, TF and PF purposes. Typically, legal counsel in Gibraltar or a CISA is involved in the establishment process and both parties must comply with the requirements under POCA including carrying out adequate CDD depending on the risk posed by the fund client.

Private funds are prohibited from being listed on stock exchanges, limiting their ability to create liquidity on secondary markets. As a result, liquidity for private fund units can only be achieved through redemption or transfer of the units. Both redemptions and transfers require the involvement of TCSPs. In the case of redemptions, they can only be made to the unit holder, for whom the TCSP must complete CDD before allocating the unit. Similarly, the transfer of units can only occur after the TCSP completes CDD on the transferee.

As private funds are registered with the GFSC but not fully supervised or caught as a relevant financial business under POCA, these were considered out of scope for the thematic review. However, any concerns or issues detected by the relevant supervisory team at the GFSC which processes the registration application for private funds, will raise these with the AML/CFT Supervision team.

ML Threat and Vulnerability

Private funds could potentially be exploited for money laundering purposes, as they provide an avenue to obscure the origin of substantial funds as investments to mask the initial subscription source. This risk is considered to be medium based on the following factors:

- private funds are not subject to the same level of regulatory scrutiny by supervisory authorities as other types of funds;
- there are limitations and requirements placed on private funds under legislation (e.g. having a limited number or category of investors);
- private funds may have complex ownership structures involving multiple layers of entities, making it challenging to trace the initial source of funds;
- private funds may employ derivatives and other sophisticated financial instruments, which can add complexity to fund flows and potentially be exploited; and
- these funds still require the use of other types of financial services which would require adequate due diligence to be carried out, including verification of the source of wealth and funds related to the investments. This additional scrutiny acts as a mitigating factor against higher risks associated with private funds.

Although there are 123 small self-registered AIFMs registered with the GFSC, 48 of these are also authorised as EIFs so they are authorised and regulated by the GFSC mitigating potential risks further. The authorisation process for EIFs involves regulatory assessment and oversight, which adds an extra layer of scrutiny for those private funds.

TF Threat and Vulnerability

Private funds can be used as a vehicle to finance terrorist activities or support terrorist organisations. Private funds, especially those which are not EIFs and register with the GFSC but have a less stringent regulatory regime, can present vulnerabilities that malicious actors may exploit for illicit purposes. The following factors are relevant to the assessment of TF risk associated with private funds:

- private funds are not subject to the same level of regulatory scrutiny by supervisory authorities as other types of funds;
- there are limitations and requirements placed on private funds under legislation (e.g. having a limited number or category of investors);
- private funds may have complex ownership structures involving multiple layers of entities, making it challenging to trace the initial source of funds;
- private funds may employ derivatives and other sophisticated financial instruments, which can add complexity to fund flows and potentially be exploited; and
- these funds still require the use of other types of financial services which would require adequate due diligence to be carried out, including verification of the source of wealth and funds related to the investments. This additional scrutiny acts as a mitigating factor against higher risks associated with private funds.

Although there are 123 small self-registered AIFMs registered with the GFSC, 48 of these are also authorised as EIFs so they are authorised and regulated by the GFSC mitigating potential risks further. The authorisation process for EIFs involves regulatory assessment and oversight, which adds an extra layer of scrutiny for those private funds.

The threat and vulnerability of TF differ slightly from ML on the basis that it is typically smaller amounts of funds that are used for raising funds for the purpose of carrying out a

terrorist attack so terrorist organisations may be less inclined to use private funds as a means of funding a terrorist attack or group.

Alternative Investment Fund Managers

An alternative investment fund manager (AIFM) is an entity that oversees and manages one or more alternative investment funds (AIFs). The responsibilities of an AIFM include the provision of fund management services, such as recording or actioning investment decisions, portfolio and risk management, asset valuation, distribution and compliance.

AIFMs are regulated by the GFSC under the Financial Services Act 2019 and are required to comply with the Financial Services (Alternative Investment Fund Managers) Regulations 2020. AIFMs are considered a relevant financial business under the Proceeds of Crime Act 2015 and therefore, authorised and supervised by the GFSC for AML/CFT/CPF purposes.

Gibraltar currently has 6 authorised AIFMs which are responsible for managing their clients' investment portfolios. There are two AIFMs which also act as Collective Investment Scheme Administrators (CISAs) and are therefore, also responsible for the oversight and collation of due diligence of the subscribers.

The main risk associated with AIFMs in Gibraltar is the over-reliance placed on the CISAs to perform the necessary due diligence, despite some of these not being locally based. The thematic review of the funds sector highlighted a lack of awareness in some of the firms concerning Gibraltar specific AML/CFT/CPF requirements within this sector. To address these concerns, the GFSC is actively working with these AIFMs to enhance regulatory standards and ensure compliance with the legislative requirements.

It was identified through the Thematic Review, that AIFMs place significant reliance on the CISA to undertake the due diligence requirements. The risk is still considered to be low on the basis that all AIFMs operating in Gibraltar have a CISA based in the European Union, which means that all fund subscribers are subject to due diligence measures similar or equivalent to those required in Gibraltar.

By working closely with the AIFMs and ensuring compliance through the CISAs, where applicable, the GFSC aims to strengthen risk management and improve overall compliance standards within the sector.

ML Threat and Vulnerability

The risk of AIFMs being used as a conduit for money laundering is considered low, primarily because these entities do not involve direct fund exchanges and their main purpose is to manage the fund portfolio and investments. One of the main risks would be if the AIFM itself establishes a fund for the purpose of cleaning or integrating illicit funds. Nonetheless, no instances of this have been found to take place in practice.

An AIFM's role is primarily focused on managing the investment portfolio and they do not usually hold sole responsibility for the oversight of subscribers within the funds. This responsibility is typically outsourced to the CISA, which acts as an intermediary between the investors and the AIFM.

The CISA is required to conduct thorough due diligence on the subscribers, ensuring that the source of wealth or funds used for investment is legitimate and complies with AML/CFT/CPF regulations. This process involves verifying the origin of the funds and assessing the risk associated with each subscriber to identify any potential ML activity.

TF Threat and Vulnerability

AIFMs are generally considered to be low risk in relation to terrorist financing. The nature of these entities, where subscription amounts are typically relatively high and often have

minimum amount requirements, makes them less attractive to terrorist organisations seeking to move smaller amounts of money discreetly.

An AIFM's role is primarily focused on managing the investment portfolio and they do not usually hold sole responsibility for the oversight of subscribers within the funds. This responsibility is typically outsourced to the CISA, which acts as an intermediary between the investors and the AIFM.

The CISA is required to conduct thorough due diligence on the subscribers, ensuring that the source of wealth or funds used for investment is legitimate and complies with AML/CFT/CPF regulations. This process involves verifying the origin of the funds and assessing the risk associated with each subscriber to identify any potential TF activity.

Collective Investment Scheme Administrators

A Collective Investment Scheme Administrator (CISA) is a firm which is responsible for the operational and administrative aspects of managing a Collective Investment Scheme (CIS). A CIS is a pool of funds from multiple investors that participate in the investment of various securities such as stocks, bonds, and other financial instruments with the same ultimate goal. The aim of a collective investment scheme is to provide diversification and professional management to individual investors and typically have a strong understanding of financial markets, different investment vehicles and regulatory and legal requirements. The main governing legislation for CISAs is the Financial Services (Collective Investment Scheme Administrators) Regulations 2020. CISAs also have a duty to ensure that the fund operates in accordance with relevant financial regulations, legislation, and guidelines. The CIS itself will, nevertheless, continue to bear ultimate responsibility over such regulatory and legislative requirements and must ensure to apply and maintain adequate oversight of the function(s) it outsources to the CISA.

A CISA has a variety of responsibilities such as the daily management of the CIS. This includes the onboarding of investors, as well as processing investors' subscriptions, redemptions, switches and transfers and maintaining accurate records and ensuring compliance with regulatory and legislative requirements. One of the main tasks the CISA undertakes is the tracking of the CIS's financial transactions which includes the calculation of the fund's Net Asset Value on a regular basis and preparation of the financial statements for investors. This mitigates ML and TF risks given that the financial statements are prepared by the CISAs who are regulated and required to implement strong internal controls to identify, assess and prevent financial crime risks from materialising.

CISAs are authorised and regulated by the GFSC and therefore, undergo a stringent fitness and propriety assessment as part of the application process. They are actively supervised by the GFSC for AML/CFT purposes in ensuring full compliance with the requirements. There are currently 9 CISAs authorised and regulated by the GFSC. The use of a CISA plays a significant role in detecting and reducing ML and TF risks that funds may face. This is because the CISA acts as a gatekeeper by implementing a variety of mitigating measures to enhance transparency in collecting appropriate due diligence, ongoing monitoring and reporting any suspicious activity. Generally, the standard of compliance observed by the GFSC across the CISAs (as assessed by way of the sectoral thematic review) is considered relatively high. CISAs in Gibraltar typically have their own investor screening, transaction monitoring and CDD procedures and thus, play a significant role in their oversight of the fund in helping to reduce the potential for ML or TF occurring within Experienced Investor Funds.

Experienced Investor Funds

An Experienced Investor Fund (EIF) is a fund specifically designed for professional, high net worth or experienced investors. These funds are often structured in a way that assumes investors have a deeper understanding of financial markets, risks and complex investment

strategies. EIFs may offer more complex investment opportunities which typically involve higher risks, and potentially higher returns. Due to its investment complexity, these funds have certain criteria that investors must meet in order to participate. This means that participants must have either a minimum level of financial assets, income or previous investment experience.

In Gibraltar, there are currently 56 regulated EIFs that fall under the supervision of the GFSC. Given the potential risks associated with financial transactions and investments, it is crucial to have safeguards in place. Gibraltar has employed various measures to address the ML and TF risks posed by EIFs. As at Q1 2024, the current assets under management for all EIFs operating within Gibraltar is £1,170,923,105. The table below demonstrates the assets under management for all EIFs from 2021 to 2024.

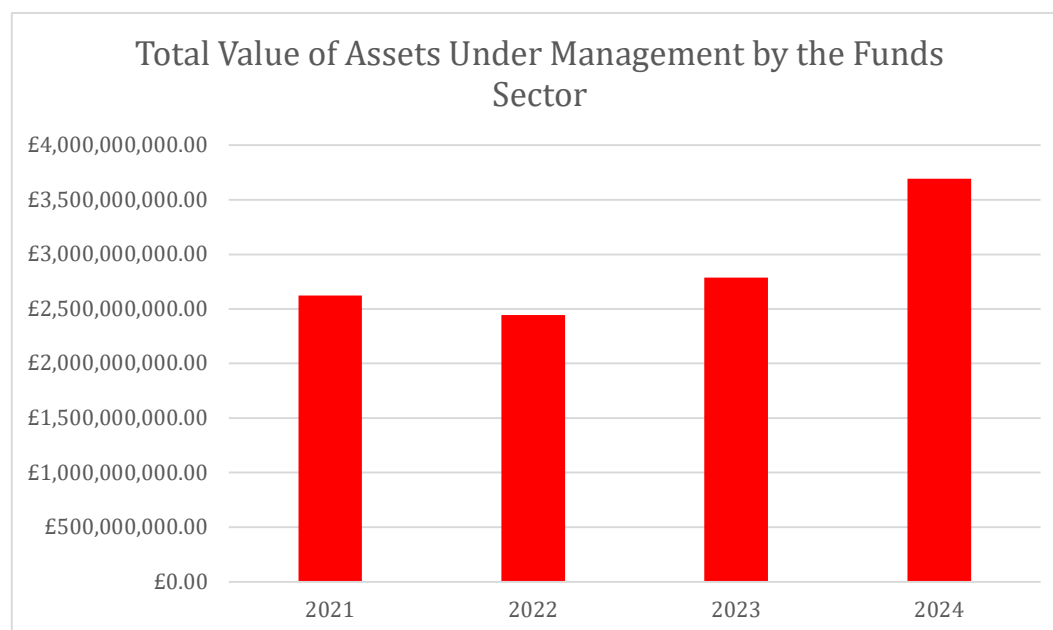


FIGURE 7 - TOTAL VALUE OF ASSETS UNDER MANAGEMENT BY THE FUNDS SECTOR

EIFs are subject to the provisions of POCA, despite compliance generally being outsourced to a CISA. An EIF is still required to ensure it has sufficient oversight over the CISA to ascertain that they are complying with all relevant legislative and regulatory requirements. It is the EIF who maintains ultimate responsibility for compliance, which is why each EIF is required to also appoint an MLRO and ensure that all AML/CFT/CPF requirements are adhered to. These measures are in place to ensure that ML and TF risks associated with the EIF can be detected and prevented effectively.

The legislation which governs the principles and requirements for EIFs is the Financial Services (Experienced Investor Funds) Regulations 2020 (EIF Regulations). An EIF may be a company formed or re-domiciled under the Companies Act 2014, a protected cell company, a unit trust established under and governed by Gibraltar law, a limited partnership, or any other form of vehicle/entity. EIFs are subject to approval by the GFSC and the EIF Regulations require all individuals responsible for management and control of an EIF to be identified. On establishment of an EIF, the entity is required to obtain a legal opinion from a lawyer that has at least 5 years of professional standing, is a barrister or solicitor of the Supreme Court of Gibraltar and is independent of the Administrator. The legal opinion is required to confirm that at the date of the entity's establishment, it complies with the provisions under the EIF Regulations.

The fund is also required to appoint a CISA, who is primarily responsible for the calculation of the net asset value of the EIF and for undertaking transfer agency services. In addition to an Administrator, the EIF is required to appoint an auditor in Gibraltar and undertake an annual audit review. CISAs and auditors also fall within the remit of the Proceeds of Crime Act 2015 (POCA) and are subject to all AML/CFT/CPF requirements under the legislation. Therefore, the CISA and auditor are obliged to report any suspicious ML or TF activity identified in the conduct of their reviews. Furthermore, under the EIF Regulations, the fund is required to appoint a minimum of two persons (EIF Directors), who are responsible for the management and operation of the fund. This is a regulated activity and each EIF Director must obtain an approval by the GFSC in order to carry out their respective director duties. The EIF must also submit its offering document to the GFSC in accordance with EIF Regulations. The offer document must disclose the fund's investment objective and investment strategy, including the EIF's approach to borrowing and leverage and any applicable restrictions. In the event where ML and/or TF is suspected, the GFSC maintains the right to intervene and take over the business of the fund.

These measures ensure to promote transparency and aim to reduce financial crime from occurring through an EIF. Given that there are numerous complexities in establishing an EIF, it is likely to deter individuals from establishing such a vehicle for the purposes of ML and TF. Once established, the EIF itself is required to comply with the provisions under POCA and there are also several independent third parties engaged by the EIF who are required to comply with POCA in respect of the EIF as their client. This provides several lines of defence in ensuring that suspicious ML or TF activity is detected and managed resulting in the use of an EIF for ML and TF purposes being less appealing to criminals. Additionally, any listings on a stock exchange to create liquidity of the units of an EIF on a secondary market, are required to be disclosed within the offering document and requires prior authorisation from the GFSC. In practice, only a very small number of EIFs have been listed on a stock exchange. Where an EIF is not listed, to liquidate a position in a unit, the holder would either redeem their unit or transfer it to a third party. In the case of redemptions, the EIF would be required to undertake ongoing CDD in respect of the investor and in the case of transfers, the EIF would be required to undertake CDD on the transferee prior to permitting the transfer of the unit. This would apply not only in respect of the provisions under POCA but also for the purposes of ensuring that the transferee satisfies the definition of an experienced investor in accordance with the EIF Regulations.

ML Threat and Vulnerability

EIFs are specialised investment vehicles designed for experienced investors. As these funds operate within a complex financial landscape, they are vulnerable to various risks related to money laundering. Some of the risks to consider with EIFs is that due to its complex investment strategies, money launderers may attempt to mask the true nature of transactions and make it difficult for authorities to detect suspicious activities. Criminals may not be transparent about the EIF's true investments strategies, making it difficult to assess the legitimacy of funds and investments. Such opacity can be exploited by money launderers seeking to inject illicit funds into the financial system. EIFs also establish relationships with various service providers, such as CISAs, TCSPs, custodians and legal advisors and there is a risk that such relationships could be potentially exploited by criminals to launder funds. Any risks which arise due to emerging technologies must also be taken into account. There is now an increased use of crypto funds in Gibraltar with the use of blockchain and cryptocurrencies, which can facilitate anonymous and cross-border transactions, creating new avenues for money laundering within EIFs.

The money laundering risks discussed above are largely diminished on the basis that there is a comprehensive framework encompassing EIFs. These funds must adhere to stipulations outlined in the EIF Regulations, POCA, the Financial Services Act 2019 and, where relevant, are

additionally subject to the well-established, regulated crypto framework established within Gibraltar, for those EIFs operating as crypto funds.

In 2022, the GFSC carried out an extensive Thematic Review of the Funds sector covering all AML/CFT requirements. The Outcomes Report revealed that, across the board, EIFs did not collect adequate source of wealth/funds on its underlying investors and that not all firms completed appropriate PEP/sanction screening on the underlying investors of the fund on an ongoing basis. Some other issues identified was a lack of ongoing monitoring, specifically where there had been a redemption or where an additional subscription took place.

These findings contribute to an environment where EIFs may become attractive vehicles for money laundering and terrorist financing activities. The lack of due diligence, screening, ongoing monitoring, and understanding of the inherent risks in EIFs can allow criminals to exploit vulnerabilities within the system. In completing this thematic review, the GFSC has had the opportunity to address these weaknesses so that firms can effectively strengthen their AML/CFT/CPF systems and controls, thus substantially mitigating the risks associated with financial crime and ensuring the integrity of the financial system. Furthermore, the GFSC is continuously working with regulated entities to address these findings and actively monitors their remediation plans to ensure these are being appropriately actioned. The undertaking of thematic reviews in combination with the regulated entities' remediation plans and the regulatory and legislative frameworks in place, significantly mitigate these risks from materialising.

TF Threat and Vulnerability

EIFs may also be susceptible to misuse for terrorist financing purposes. Many of these risks would be as a result of non-compliance with regulatory and legislative requirements as those set out above, such as, the lack of ongoing monitoring of transactions and business relationships, lack of sanctions screening. Given that most EIFs in Gibraltar are managed by CISAs and TCSPs, there is a further layer of protection for EIFs as the CISAs and TCSPs typically implement a variety of mitigation strategies in order to address the identified vulnerabilities and threats that EIFs may face. In combination with the use of CISAs as well as the fact that the EIF itself must also appoint an MLRO and ensure that it complies with all AML/CFT/CPF requirements, the risk of EIFs being used as a vehicle to funnel illicit funds into the financial system for terrorist financing purposes is reduced.

The tables below demonstrate the low level of customers and funds which derive from conflict zone jurisdictions. The likelihood of funds being used as a vehicle for terrorist financing in Gibraltar is low. All EIFs generally have a minimum time for subscription and therefore requesting to redeem these funds before the maturity date usually incurs a penalty. All fund administrators within Gibraltar conduct ongoing monitoring at the time of redemption of funds thus mitigating this risk further and supporting the low risk level of TF locally.

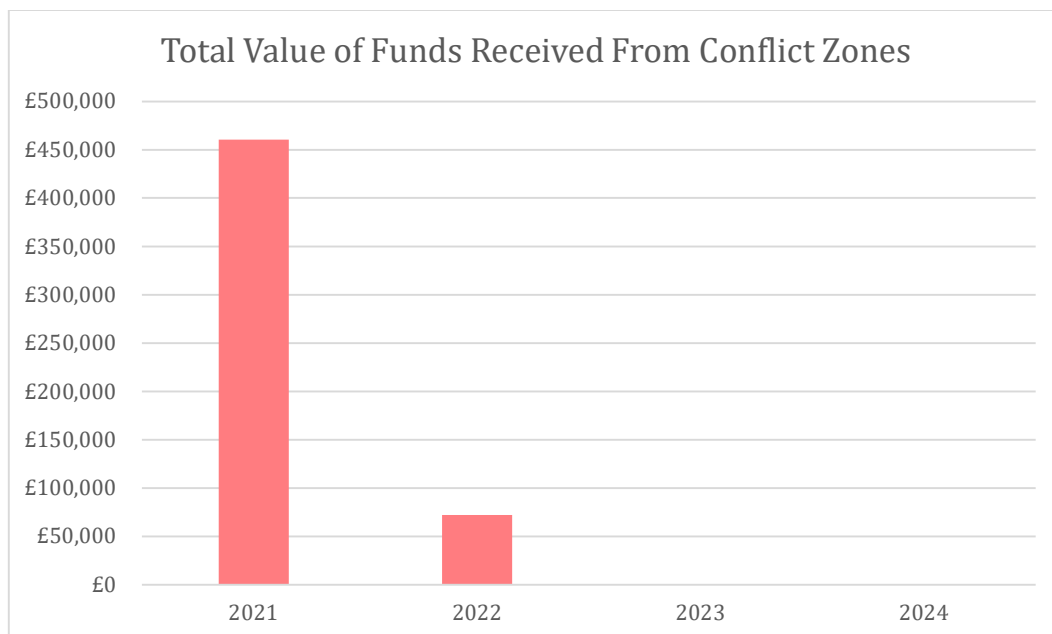


FIGURE 8 - TOTAL VALUE OF FUNDS RECEIVED FROM CONFLICT ZONES FUNDS SECTOR

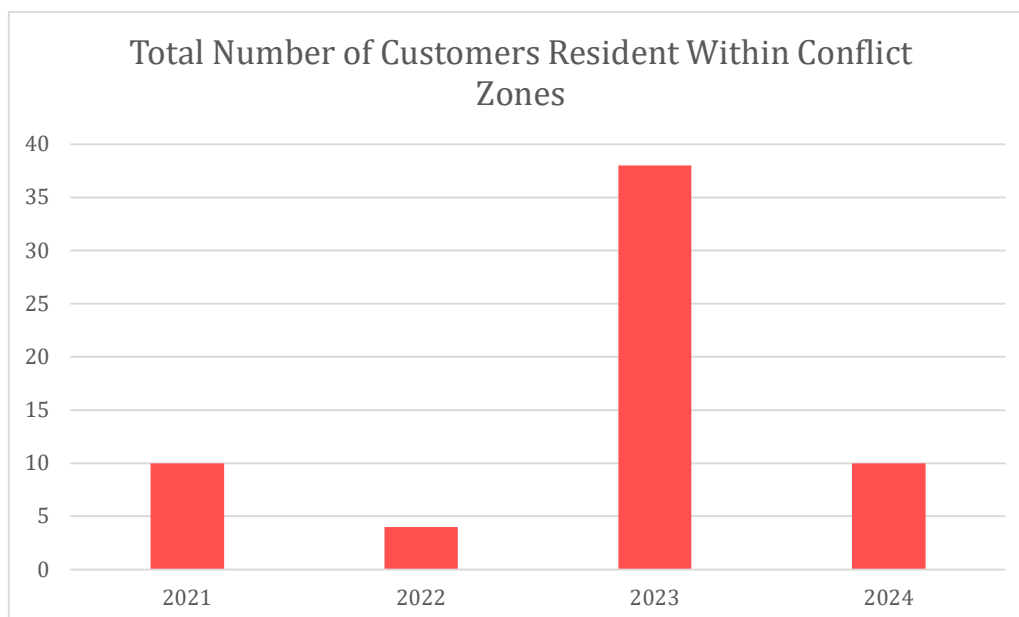


FIGURE 9 - TOTAL NUMBER OF CUSTOMERS RESIDENT WITHIN CONFLICT ZONES

7.6 E-Money

E-money is defined under the Financial Services Act 2019 as “storing funds, including magnetically, as monetary value represented by a claim on the electronic money issuer which is issued on receipt of funds for the purpose of making payment transactions and is accepted by a person other than the electronic money issuer”.

Initially e-money, as a regulated concept, was created primarily to cover payment instruments that had value pre-loaded on them. However, in Gibraltar, the primary service of Electronic Money Institutions (EMIs) permits the payment instruments to be attached to an underlying payment account offered by the issuer.

Composition and size of the Financial Sector - Electronic Money Institutions (EMIs)

Number of EMIs licensed/registered in the country, of which:	3	
have branches and subsidiaries abroad	1	Malta
Total number of EMI agents or e-money distributors (of the EMIs licensed domestically)	3	United Kingdom
	2	United States
	1	Gibraltar
Cross-border transactions		
Total number of clients	1,037,744	
Total number of payment transactions	169,943,277	
Total value of payment transactions	£4,297,427,046	

TABLE 25 - MATERIALITY OF THE E-MONEY SECTOR AS AT DECEMBER 2024

Gibraltar based E-Money firms are authorised and subject to the Financial Services Act 2019, the Financial Services (Electronic Money) Regulations 2020 and the Proceeds of Crime Act 2015. All authorised E-money firms operating from or within Gibraltar are required to be authorised and regulated by the GFSC.

There are three e-money institutions operating from or within Gibraltar. Two of the three were authorised by the GFSC in 2023. The other, long-standing e-money institution has undergone regular visits where only minor findings have been identified.

Since the UK's exit from the European Union, e-money issuers within Gibraltar are only able to passport into the United Kingdom. This has somewhat mitigated the risk of money laundering and terrorist financing taking place via a Gibraltar based e-money firm as it limits the geographical exposure.

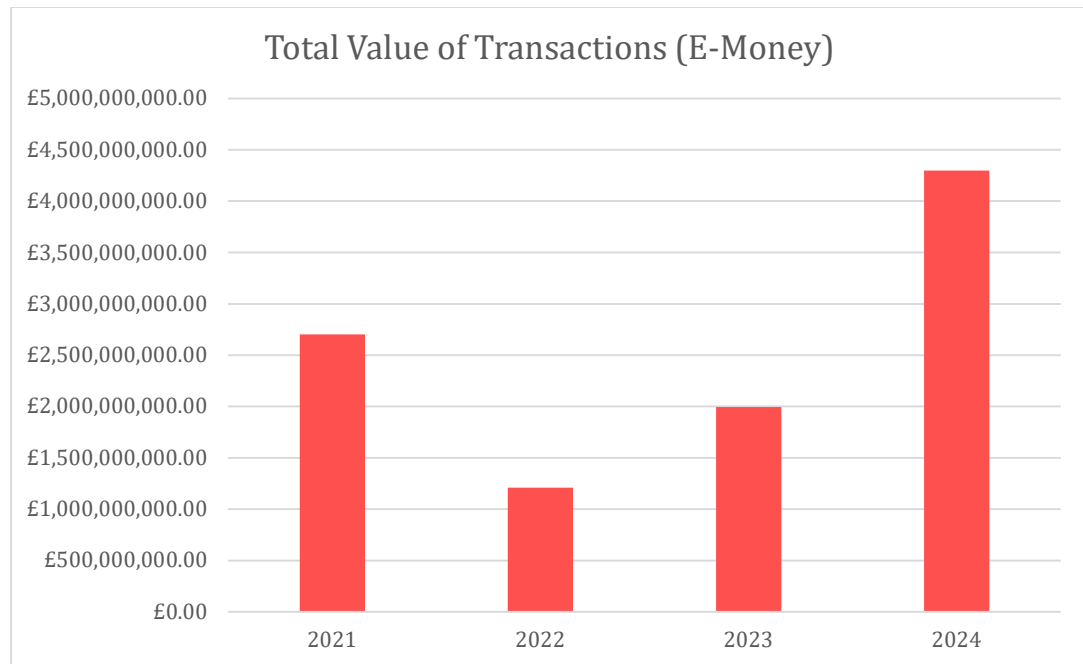


FIGURE 10 - TOTAL VALUE OF TRANSACTIONS OF THE EMONEY SECTOR

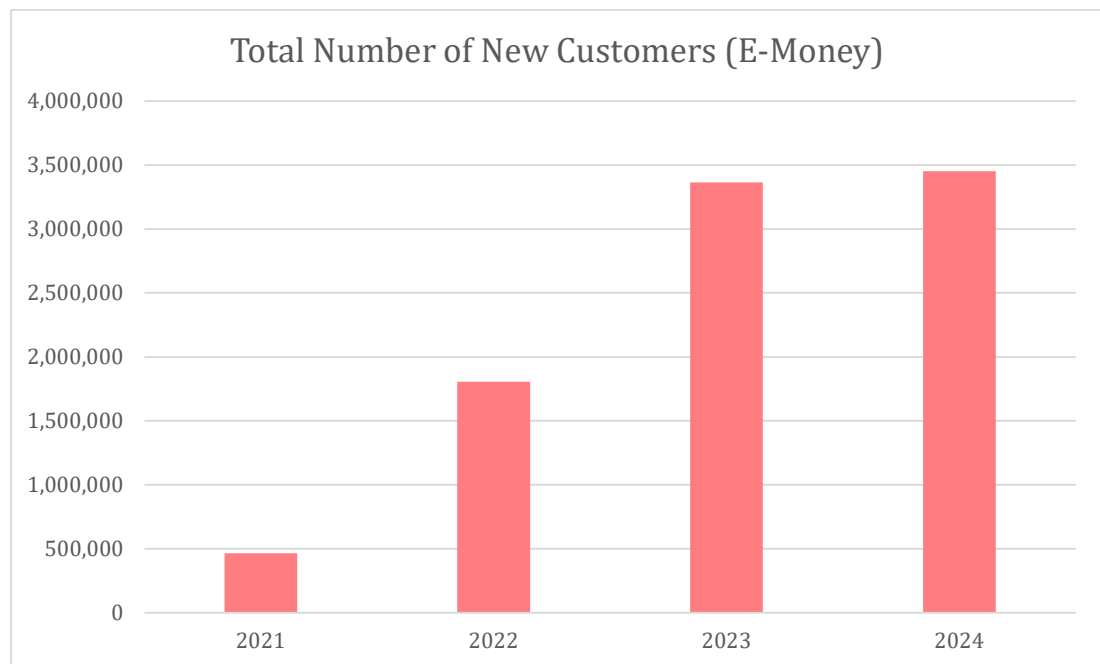


FIGURE 11 - TOTAL NUMBER OF NEW CUSTOMERS IN THE EMONEY SECTOR

E-money can be stored in various ways, such as on cards, mobile devices, and online accounts.

In the case of hardware-based products, the purchasing power resides in a personal physical device, such as a chip card, with hardware-based security features. Monetary values are typically transferred by means of device readers that do not need real-time network connectivity to a remote server.

Most of the e-money issued is software-based and effectively links a card (whether physical or accessible on a mobile phone or computer) to a regulated payment account. To enable the transfer of monetary values, the payment instrument typically needs to establish an online connection with a remote server that authenticates the transaction based on funds held in the underlying payment account. Other potential distinctions between e-money products can include how the e-money is created or issued. The key distinction relates to whether e-money can be prepaid by the user (payer) or by a third party on behalf of the payer. Gibraltar's EMIs generally offer a range of products, such as corporate expense cards and personal use cards. Gibraltar prohibits the use of anonymous e-money products which acts as a mitigating factor against potential illicit activity. The number of e-money issuers and types of products/services offered has changed since 2020. This is largely down to the impact of Brexit where several e-money institutions moved to other jurisdictions within the EU and so, local e-money institutions are now only able to offer services to the UK market.

How e-money products are classified depends on whether the product is multifunctional or is linked to a platform. Both types can be used online, but the latter only allows purchases in a single platform and does not allow peer-to-peer transfers. In both cases, a bank account is needed for loading the e-money products. This reduces the risk as the loading channel is a regulated bank which will have been required to conduct full due diligence requirements on the client and will have knowledge of the source of funds used. In addition, there are types of e-money cards which are single use and non-reloadable. These usually require minimal due diligence requirements owing to the fact that they are not reloadable and will be disposed of once the pre-loaded funds have been spent. A mitigating factor is that anonymous cards are not permitted under Gibraltar law. Therefore, all e-money products sold from or within Gibraltar will have some level of due diligence conducted on the individual/corporate who will be utilising the product.

There are different parties involved in e-money issuance which fall within scope of the Financial Services (Electronic Money) Regulations 2020:

- **the issuer:** an entity which issues e-money to the customer (whether a consumer or a business) in exchange for payment. It is the entity that requires authorisation to issue electronic money and is regulated by the GFSC;
- **the distributor:** an entity other than the issuer that can distribute or redeem e-money on behalf of the issuer (i.e. it provides a means of distribution for the e-money issued by the issuer, such as a retail outlet selling prepaid cards);
- **the agent:** an entity that acts on behalf of the e-money issuer, enabling an issuer to carry out ancillary payment services activities (except for issuing e-money).

Within Gibraltar, there are some EMIs which work with other businesses to offer branded cards under a program manager agreement. The EMI will outsource some of its AML/CFT functions to the program manager, such as customer due diligence and ongoing monitoring. The program managers themselves are generally not regulated entities and therefore rely upon the permission of the EMI to issue these types of payment instruments. The EMIs retain ultimate responsibility in ensuring compliance with legislative and regulatory requirements and this is assessed and verified by the GFSC through its ongoing supervision of the E-money sector.

Open Loop

Open loop cards are cards that can be used at any retailer or merchant and in some cases, at ATMs for cash withdrawals. There are various types of e-money products which operate as 'open loop' cards. These are attached to a card scheme and allow the user to purchase products in locations where that card scheme is accepted. The majority of e-money products are also reloadable. E-money issuers allow their clients to top-up additional funds from different loading channels, such as from a credit/debit account in the user's name via bank

transfer and in some instances in cash. There are also e-money products classified as single use cards, e.g. gift cards which are non-reloadable and can be used only at a specific retailer. However, gift card options represent a small share of products available in Gibraltar so this is not a significant risk.

It is also important to note that any distributors of e-money appointed by the EMI must have processes in place that ensure the EMI is able to meet its relevant AML/CFT obligations, and they must be notified to the GFSC.

There are currently three authorised e-money institutions in Gibraltar which offer open-loop products. The cross-border nature of e-money products naturally increases an entity's exposure to high-risk jurisdictions, however, the risk is mitigated via the GFSC's assessment of the implementation of legislative and regulatory requirements which forms part of its ongoing supervision via off-site and on-site reviews.

Closed Loop

Closed loop cards are prepaid cards which can be used to purchase goods and services within a single network, or limited network of service providers. These cards are split into various categories such as those which are single use and those which can be used to acquire cumulative purchases. The difference between the cards is that single use cards would be topped up initially with a limited load value and then disposed of. Providers who offer cards that are used to make purchases on an ongoing basis would subject their clients to due diligence measures for the purposes of repayment.

There is minimal risk associated with closed loop cards given the limited network in which they can be used. This being said, for single use cards the primary loading could be cash-based. Closed loop cards are out of scope of the legislation.

ML Threat and Vulnerability Assessment

The money laundering threat posed by e-money primarily arises because of some cash-based products that can be used by criminal organisations. E-money products have some advantages over cash when it comes to moving that money using peer-to-peer transfers among customers on the same platform, with a view to create multiple layers from the origin of the funds. Internationally, financial intelligence units have detected multiples cases of misuse of e-money (tax fraud, drug trafficking, prostitution) through the purchase of multiple prepaid cards. Law enforcement agencies have found cases where the proceeds of drug trafficking were laundered by prepaid cards.

Among the range of e-money products, the products most exposed to money laundering risks are the ones that allow cash deposits, however, these are uncommon in Gibraltar so the risk is minimal. The use of these products for money laundering purposes is costly for perpetrators because of the lower thresholds and the cost of hiring individuals to circumvent the thresholds for applying customer due diligence. However, when some intermediaries act in the delivery channel of the e-money product (distributors/agents), this can often be the weakest part of the AML prevention framework if firms are unable to perform efficient monitoring of their distributor's network. It is worth noting that the current agents and distributors can only passport into Gibraltar from the UK due to the UK's exit from the European Union, therefore, the risk is reduced.

. Furthermore, there is no evidence of these practices happening locally, nor deficiencies identified in the EMIs oversight of their network of distributors/agents. Therefore, the risk is considered to be mitigated in this respect.

Terrorist Financing

Transporting value to conflict zones or high-risk jurisdictions.

E-money products while not permitted to be anonymous in Gibraltar, may offer perceived advantages over cash for terrorist financing purposes. The relatively low transaction amounts often associated with terrorist financing align with the typical usage patterns of e-money, potentially making it an attractive option for such activities. Additionally, the remote, non-face-to-face nature of e-money transactions could appeal to individuals seeking to avoid scrutiny. However, the traceability of e-money transactions, particularly those linked to bank accounts, presents an obstacle to its use for illicit purposes.

Most of the e-money products are also linked to a payment account, facilitating the use of bank transfers as an additional loading/payout channel. The risk of terrorists using e-money products for related services, such as car rental, is mitigated to an extent by the fact that prepaid cards are at times, not accepted in order for the retailer to avoid insufficient funds fraud.

Despite these mitigating factors, the inherent risk of e-money products being used for terrorist financing purposes cannot be entirely dismissed. The existence of multiple loading channels, and the ability for low value transactions to go undetected means that it requires consistent monitoring, sufficient thresholds and human intervention to be in place to detect any unusual activity.

When assessing the terrorist financing threat of e-money, additional considerations need to be made relating to transactions undertaken in “conflict zones”. These regions are defined as directly experiencing or adjacent to areas of war or extreme violence. When perpetrators attempt to send money to conflict zones, e-money products can often be seen as a more viable alternative but using them as a means of payment in those countries can be more complicated or restrictive than cash. The obligation for regulated entities to apply customer due diligence measures and transaction monitoring thresholds, presents itself as an additional barrier to its usage for illicit activity.

Despite the traceability of payments, perpetrators can still use these products as a means of payment even if they have to undergo customer due diligence measures. Data obtained through the GFSC’s Annual Financial Crime Supervisory Return suggests that e-money transactions related with a number of conflict zone jurisdictions constitutes 0.74% of the total number of e-money transactions carried out, demonstrating the low exposure and risk to conflict zones. Additionally, this is further mitigated by the fact that anonymous e-money products are not permitted in Gibraltar under its legislative framework.

	2024	2023	2022	2021
% vs total volume	0.16%	1.61%	0.03%	0.30%

TABLE 26 - E-MONEY SECTOR: FUNDS RECEIVED FROM HIGH-RISK COUNTRIES & CONFLICT ZONES

The above table demonstrates the relatively low volume of transactions and funds received from high risk jurisdictions or conflict zones. It should be noted that the increase in exposure from 2022 to 2023 relates primarily to a singular conflict zone jurisdiction (Israel). The relatively low level of exposure year on year.

7.7 Virtual Asset Service Providers (VASPS).

The sector’s engagement with competent authorities and law enforcement agencies is crucial to improve efficiency and mitigate such risks and reliance on technology improves efficiency in identifying suspicion, particularly where high-risk countries are involved. The role of the

GFSC in supervising these firms and ensuring that adequate controls are in place fulfils this function. Virtual Asset Service Providers (VASPs).

As an emerging product in the financial services sector, virtual assets (VAs) present new potential risks and vulnerabilities to ML, TF and PF. VAs are a digital representation of value that can be digitally traded or transferred and can be used for payment or investment purposes. It is important to note that these are not considered to include digital representations of fiat currencies or financial instruments.

Composition and size of the Financial Sector - VASP Sector (for the purpose of this exercise, VASPs form part of the financial sector)

Total number of VASPs of which:	30 total authorised/registered VASPs
Also have financial institution's licence (registration)	0
Other type of licence	1 (Banking permission)
Number of transactions	57,219,232
Total value of transactions	£186,912,278,574
Total number of clients	5,821,628

TABLE 27 - MATERIALITY OF THE VASP SECTOR AS AT 31 DEC 2024

All VASPs are subject to the supervision of the GFSC. VASPs are required to seek authorisation under either the Distributed Ledger Technology (DLT) framework or registration under the VASP framework. The regulatory regime that a particular VASP is subject to, is dependent on the nature of its products and services. The scope of the VASP registration framework has been set out within the GFSC'S [VASP Registration Scope Guidance Note](#). In total, the GFSC has 30 supervised VASPs that are either authorised or registered to provide VA-related services.

In 2018, Gibraltar implemented a regulatory framework capturing any entity carrying out by way of business, in or from Gibraltar, the use of "DLT for storage or transmission of value belonging to another". Entities conducting this activity are required to be authorised by the GFSC as a DLT Provider. DLT Providers are required to comply with 10 key regulatory principles, of which Principle 8 relates to the prevention of financial crime. DLT Providers authorised in Gibraltar offer a range of VA services including:

- Exchange services;
- Over-the-counter (OTC) exchange services;
- Custodial services; and
- Leveraged trading services.

The VASP registration regime was subsequently established in 2021 following a gap analysis undertaken between the DLT framework and the FATF definition of a VASP. The review concluded that the definition of a DLT Provider falls within the FATF's VASP definition, however, the FATF definition was identified as wider than that of a DLT Provider. The following additional VASP activities were identified as falling outside of the DLT framework, and are now required to seek registration with the GFSC for AML/CFT/CPF supervision purposes:

- Token sales; and
- Non-custodial exchanges & arrangers.

Criminal actors may consider VAs an attractive means to facilitate financial crime, as the provision of VA services is typically characterised by non-face-to-face transactions that can offer a higher degree of anonymity than traditional non-cash payment methods (due to a lack of uniform regulatory oversight across jurisdictions). In Gibraltar, however, this is largely

mitigated on the basis that all VASPs are subject to AML/CFT/CPF supervision by the GFSC. The standard of compliance against AML/CFT/CPF-related requirements across the sector is generally quite high, with an observed decrease in the number/significance of deficiencies identified by the GFSC by way of its onsite inspections. The DLT/VASP sector has been one of the highest reporting sectors in terms of SARs, further demonstrating the standard of controls and awareness maintained in the sector.

YEAR	NO. SARs RAISED BY VASP SECTOR	PROPORTION OF TOTAL SARs RAISED	PROPORTION OF TOTAL SARs RAISED (EXCLUDING E-GAMING)
2020	343	15.12%	23.37%
2021	426	10.81%	63.11%
2022	291	8.31%	47.70%
2023	815	16.67%	60.32%
2024	1,591	30.34%	72.67%

TABLE 28 - SARs RAISED BY VASP SECTOR

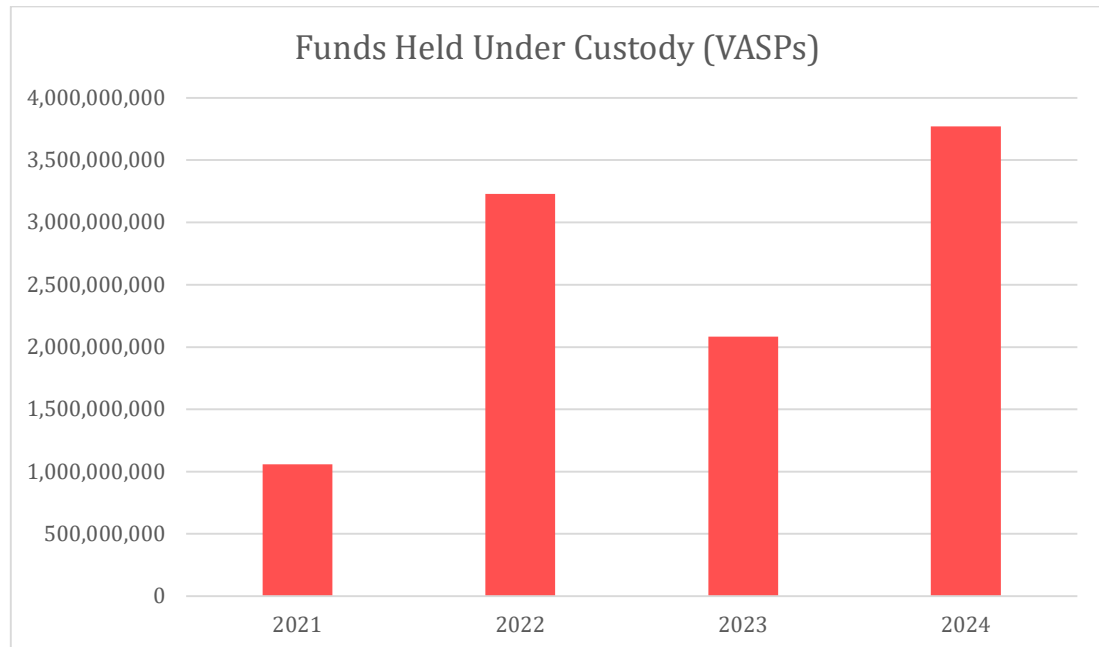
Less than 10% of entities within the other financial services sectors regulated by the GFSC, indicated that they have had exposure to VAs within the Annual Financial Crime Return. The vast majority of these entities are collective investment schemes which hold a portion of their investment portfolio in VA currencies. This demonstrates the limited exposure to VA-related risks associated with the remainder of Gibraltar's financial services industry outside of the VASP sector.

Custodial Exchanges

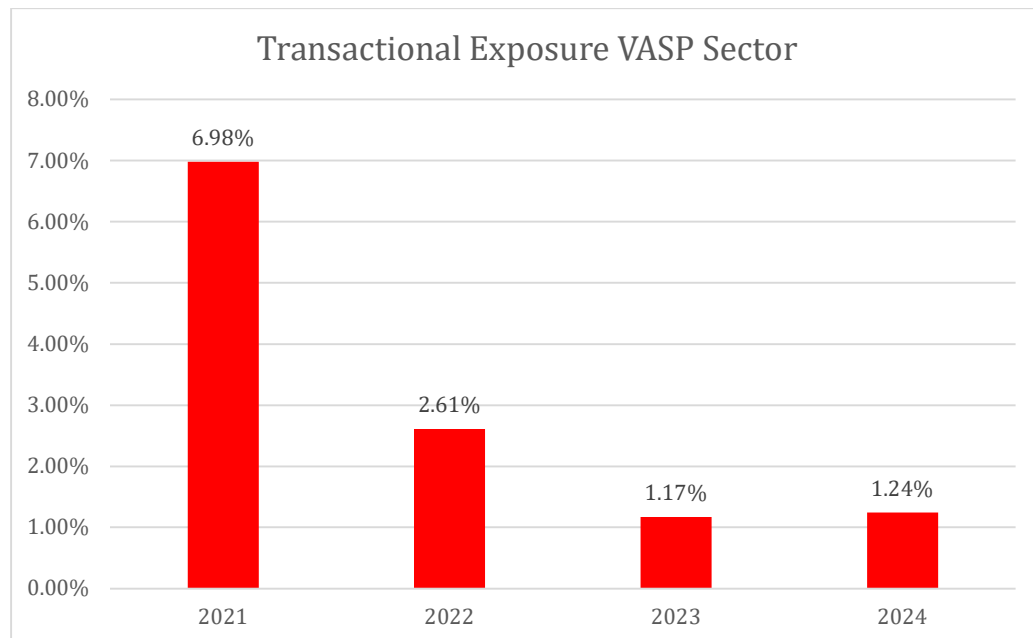
VA exchange platforms facilitate the buying, selling and trading of VAs. Such platforms may accept a wide array of payment methods, including both fiat and virtual currencies. Custodial exchanges will facilitate the execution of each trade by storing or transmitting the assets which are the subject of the transaction. This activity therefore falls within the scope of the DLT framework and is subject to authorisation and supervision by the GFSC. As at 31 December 2024, there were 9 DLT Providers authorised for the provision of custodial VA exchange services.

VA exchange services are typically offered in tandem with custodial services, where the VASP in question will hold and manage a user's funds on their behalf. Like traditional currency exchanges, VA exchanges also provide an overall picture of movements in a particular asset's exchange price and volatility.

VA exchanges are at risk of facilitating ML & TF primarily on the basis that they enable the swift execution of transactions at high volumes and values. Illicit actors may consider this an appealing means of facilitating the complex movement of funds in a manner that obscures their true origin. Perpetrators may also seek to convert VA funds of illicit origin to fiat currency, or another more favourable VA currency. Since 2020, the data collected by the GFSC through its Annual Financial Crime Return demonstrates that the number and value of transactions facilitated by the sector has increased significantly, presenting an increased level of potential risk exposure. As demonstrated in the figure below, this is mirrored by an overall increase in the value of funds held under custody by the sector. This is somewhat mitigated, however, by the standard of AML/CFT/CPF controls applied within the sector which is generally satisfactory.

**FIGURE 12 - FUNDS HELD UNDER CUSTODY BY THE VASP SECTOR**

Exchange services also facilitate cross-border VA transactions, presenting a potential means for perpetrators to move illicit funds across jurisdictions. Despite the overall increase in transactional activity in the sector, the proportion of funds issued to or received from higher risk jurisdictions has decreased (8.76% of total transactional value in 2020 versus 2.61% in 2022). This lowers the potential risk profile associated with the cross-border movements of funds enabled by the sector.

**FIGURE 13 - PROPORTION OF TRANSACTIONS ISSUED TO/FROM HIGH RISK JURISDICTIONS**

In recent years, evidence has shown a significant increase in the number of VA exchanges targeted by and subjected to cyberattacks. Cybercrime is used as a means to gain custody of assets held by a particular exchange, to then launder the stolen funds or use them for the purposes of funding criminal activity. Principle 7 of the GFSC's DLT Framework requires that a DLT Provider "must ensure that all systems and security access protocols are maintained to appropriate high standards". DLT Providers are closely supervised by the GFSC against the application of appropriate cybersecurity measures, mitigating the potential risk of a cyberattack. The standard of controls applied by the sector in relation to cybersecurity and business continuity are assessed as high.

Non-Custodial Exchanges & Arrangers

As of 2021, the exchange or arrangement with a view to exchange, of virtual assets for money, money for virtual assets, or one virtual asset for another, are subject to a VASP registration regime. In order to provide guidance as to the scope of the VASP activities caught under the VASP registration regime, the GFSC has published its [VASP Registration Scope Guidance Note](#).

The primary business model that falls under this category is that of a non-custodial over-the-counter (OTC) exchange or brokerage desk, where the entity facilitates the exchange without directly storing or transmitting the VAs which are the subject of the transaction. Due to the instantaneous and irreversible nature of the transactions processed globally, the threats and vulnerabilities related with ML/TF are similar to those faced by custodial exchanges. As at 31 December 2024, there are three entities registered with the GFSC to provide this service.

Wallet Providers

A VA "wallet" is a software application or hardware device that allows a user the ability to store, manage and interact with its VAs. Users may store VAs on their own personal device or entrust a wallet provider to hold and administer for them on their behalf. Access to a particular wallet is secured and maintained through a user's "keys", i.e. a cryptographically encrypted data set used for the purposes of restricting access.

There are three main types of VA wallet:

- Hardware wallets – Physical devices designed to securely store VAs entirely offline;
- Software wallets – Applications or software programs installed on a device (such as a desktop or smartphone) which provide users with software applications that allow them to view their transactional history, send and receive virtual assets, and interact with blockchain networks; and
- Custodial wallets – Wallets provided as a service by a third-party, which take custody of a user's private keys on their behalf. This can be considered analogous to a traditional credit institution providing a personal bank account.

VAs can either be stored via an online (hot storage) wallet, or offline (cold storage) wallet. Each approach to VA storage has a significant impact on the potential security considerations associated with the assets in question. Although less easily accessible to the primary user, cold storage is typically considered more secure on the basis that it is entirely disconnected from the internet and therefore less susceptible to hacking and cyberattack-related theft. Criminals have also been found to misuse custodial services in order to store funds across a wide array of wallet addresses, increasing the complexity associated with a particular transaction or the ownership of a particular set of assets.

The provision of custodial wallet services falls within scope of the DLT regulatory framework and is therefore subject to authorisation and supervision by the GFSC. As of 31 December 2024, there are 10 authorised DLT providers, 8 of which are authorised for the provision of custodial wallet services. The GFSC's Annual Financial Crime Return shows that the value of

VAs held under custody by these entities has increased significantly since 2020 as the sector has continued to mature. This increase in value may increase the sector's potential exposure to risk, however, this remains significantly mitigated as a result of the GFSC's supervisory measures.

Mining

VA mining is the process by which new units of VAs are generated. There are various means through which a "miner" can generate VAs, dependent on the particular blockchain or VA in question. The original method of mining associated with Bitcoin is that of "proof of work", in which miners solve a complex mathematical puzzle, which in turn validates transactions on the blockchain. "Proof of stake" is another common method used, in which validators (referred to as "stakers") validate transactions based on the number of VAs they hold and are willing to "stake" as collateral. Although this model does not provide a viable money laundering mechanism, it is a method that illicit actors can use to generate revenue.

Due to the decentralised nature of mining operations, limited information is available to authorities on the users involved in the validation of VAs. As newly minted VAs are not easily linked to an individual, mining VAs is an attractive target for criminal organisations, sanctions circumvention and those looking to avoid law enforcement or intelligence agencies. In recent years, there has been a significant increase in the scale and scope of illicit activity targeting the VA mining process.

"Cryptojacking" is a term used to refer to the unsanctioned use of another individual/party's mining device for the purpose of generating funds. This activity is typically associated with the use of malware or other forms of cyberattacks to make use of the processing power of a third party's device.

The use of commercial mining facilities has grown in recent years and may be exploited for illegal activity due to their capability to provide a significant and relatively anonymous revenue stream. Mined VA can then be moved across jurisdictions through peer-to-peer transactions and potentially converted to fiat currency to fund illicit operations. In order to be successful, large-scale mining operations require access to stable and cheap power, high-speed internet, and are preferably based in regions with low temperature, which can help operators avoid substantial cooling costs.

Remote mining services could be an alternative solution to the rising costs of specialised mining equipment, as well as the need for cheap power and stable internet infrastructure. Host mining facilities, for example, allow remote customers to purchase mining rigs hosted in an entirely separate location. Operators of remote mining services may be unaware of their client's identity or whether they are acting on behalf of a third party. Some commercial mining facilities also offer cloud-based mining services, where users can lease equipment and computer time.

There are no known mining pools or operations based in Gibraltar. "Proof of work" mining is not considered an attractive operation from Gibraltar given the high demand for electricity and substantive processing power required. Likewise, no cases of "cryptojacking" or other forms of fraudulent or criminal activity associated with VA mining have been identified locally. Therefore, we do not consider there is any risk exposure.

Virtual Asset Automated Teller Machines (ATMs)

VA ATMs facilitate the exchange of fiat currency to VAs, VAs to fiat currency or other forms of VAs via physical electronic terminals. Some jurisdictions consider the use of VA ATMs as an occasional transaction or similar, with resulting consequences for CDD obligations. The threats typically associated with ML and TF can be significant as VA ATMs may be potentially used to convert illicit cash into VAs or withdraw cash in other jurisdictions without passing

rigorous identity controls. In Gibraltar, the operation of a VA ATM would fall within the scope of the DLT regulatory framework and would therefore require authorisation and supervision by the GFSC mitigating the risk posed substantially. Currently there are no VA ATMs present in Gibraltar reducing the risk further.

Initial Coin Offerings

One of the primary methods used to distribute VAs is through an event commonly referred to as an Initial Coin Offering (ICO) or token sale. This involves the generation and sale of a pre-defined number of VAs (usually in the form of tokens) in exchange for fiat currency or another VA. ICOs are generally a means to raise funds for the development of a digital platform, software or otherwise participate in a particular project.

Non-fungible tokens (NFTs) are one of the emerging products in the VASP sector. There are several vulnerabilities associated with NFTs, such as subjective pricing, high-value transactions, easy transferability of ownership, the absence of a physical transfer of the asset and the exposure to online theft. Although the FATF guidance states that not all NFTs fall within the virtual asset definition, the Gibraltar Financial Services Commission has adopted a more conservative approach in considering the requirement of registration of the sales of NFTs on a case-by-case basis. In practice, the GFSC has found that in most cases, the NFT entities have been required to apply for registration.

The activity of an ICO falls within the remit of the GFSC's VASP registration framework and is therefore subject to the GFSC's registration and supervisory frameworks for AML/CFT purposes. Since the inception of the VASP registration regime in 2021, a total of 26 entities have been registered in Gibraltar for the purposes of conducting a token sale. Of these, 65% have conducted a private sale, 26% both private and public, whilst 8% conducted a public sale only. 8 of the registered token sale entities have since gone on to complete their respective sale and deregister.

The exposure to ML and TF risks is dependent, in part, on the nature of the sale in question. A token sale can be addressed to limited number of selected investors (private sale) or to the public at large (public sale). Due to the wider reach and number of investors typically associated with public sales, the risk of receiving illicit funds is considered significantly higher than that of a private sale.

Peer-to-Peer Lending

VA lending offers superior rates for users. Due to the volatility of VAs, however, borrowers using peer-to-peer (P2P) lending services must collateralise large amounts of assets, making borrowing inaccessible to the average user. Stablecoins, which are typically pegged directly to a stock of commodity or currency, provide a solution to the overcollateralization problem on the basis that they have a stable price, so there is a reduced risk of the stablecoin collateral dropping below the value of the loan. Because of this, there is a huge demand for stablecoin loans.

The provision of P2P lending services falls within the remit of the DLT regulatory framework and is therefore subject to the authorisation and supervision of the GFSC. At present there are no DLT Providers in Gibraltar actively providing such services. The risk is therefore considered minimal.

Anonymity-Enhancing Assets & Services

Anonymity-enhancing services allow for the concealment of identification information by facilitating the non-disclosure of user identity or obscuring VA transaction details. Certain VAs or blockchain protocols may themselves be privacy-enhancing in nature, allowing for the obfuscation of the identity of the sender, recipient, holder and/or beneficial owner of the VAs

in question. These assets/protocols therefore present an appealing means through which illicit actors may transfer funds on the blockchain while obscuring their identity and/or the origin of the assets.

“Mixing” or “tumbling” services provide another means through which VAs transactions can be anonymised. These services pool together various transactions in order to obfuscate the origin of particular VAs, allowing for increased anonymity. These techniques are typically associated with obscuring the identification of “tainted” VAs associated with illicit flows or services, such as in the case of stolen funds.

The GFSC’s [VASP Registration Scope Guidance Note](#) clearly notes that anonymity-enhancing products and services fall outside of the GFSC’s risk appetite as a supervisory authority and would therefore not be permitted to be registered or authorised. In the case of privacy-enhancing VAs, the GFSC does not allow these to be exchanged or listed unless express consent is provided and the privacy-enhancing feature of the asset has at no point been or would be activated. There are no known entities providing anonymity-enhancing VA services in or from Gibraltar, therefore, the level of vulnerability is considered low.

Decentralised Finance

Decentralised financial service offerings (typically referred to as “DeFi”) differ from that of their centralised counterparts in that there is no central governing body responsible for their operation. DeFi arrangements leverage on smart contracts and blockchain protocols to facilitate the provision of a wide range of financial services on a peer-to-peer basis. In many cases, however, DeFi arrangements are found to be decentralised in name only, are in fact managed by a central group of entities/individuals.

The FATF’s Targeted Update on Implementation of the FATF Standards on VAs & VASPs cites a significant level of growth in the DeFi market in 2022 & 2023, following the high-profile collapse of a well-known cryptocurrency exchange. The Targeted Update makes reference to a potential increase in the misuse of DeFi operations by criminals, particularly in relation to ransomware attacks, theft, fraud, scams, drug trafficking and proliferation financing.

In practice, the service offered by a particular arrangement in or from Gibraltar would determine the regulatory regime that the arrangement would be subject to (irrespective of the manner in which they are decentralised). Currently there are no VASP operations (or otherwise) in Gibraltar that are, or purport to be, decentralised. The level of risk associated with DeFi operations in Gibraltar is therefore low.

ML Threat and Vulnerability Assessment

By having established a full regulatory framework for the VASP sector, Gibraltar has substantially mitigated the inherent risk associated with VASPs. As set out above, the standard of compliance maintained by the VASP sector is generally quite high. Among the VA related services, privacy-enhancing assets pose a higher ML risk, however, local regulated entities do not list these products.

In terms of vulnerabilities, the instantaneous and irreversible nature of virtual asset transactions, along with peer-to-peer transfers may facilitate the creation of multiple layers to conceal the origin of funds. The vast majority of business relationships held by local VASPs are established on a non-face-to-face basis, presenting an increased risk of impersonation or falsification of identity. These factors, together with the cross-jurisdictional transactional exposure associated with the sector presents an increased level of assessed risk. As the VASP sector continues to be the main reporting sector after the Gaming sector, the perceived vulnerability of the sector remains high. While the number of SARs raised by the sector has increased together with its activity, so has the proportion of SARs raised in relation to ML suspicions (increasing from 5.97% of total SARs in 2020 to 37.13% in 2022). As identified by

the GFIU, the UK is the primary jurisdiction for the location of the suspicious activity which has been reported, whilst there were only two SARs disclosed with nexus to Gibraltar.

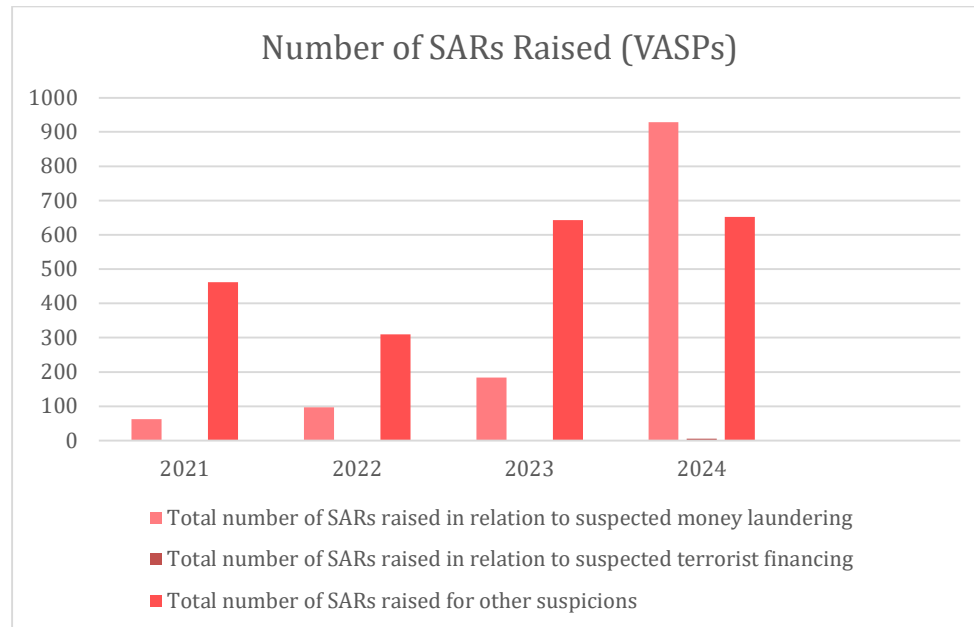


FIGURE 14 - NUMBER AND TYPE OF SARs RAISED BY VASP SECTOR

TF Threat and Vulnerability Assessment

The speed and frequency at which VA transactions can be undertaken, together with the cross-border nature of VA services continue to present a high inherent level of vulnerability to TF. As the VASP sector has continued to grow internationally, an increasing number of TF cases related to VAs have been identified. As a newer sector, however, it is likely that TF typologies will continue to develop and change over time.

The AML/CFT/CPF supervision of all VASPs by the GFSC largely mitigates the perceived level of TF risk. This risk is further mitigated when considering that the value of all transactions issued to or received from higher risk jurisdictions in 2022 amounts to 2.61% of the total transactional value facilitated by the sector. This is corroborated by the fact that in 2023, and 2024, only two SARs were raised by the DLT/VASP sector relating to potential TF activities. The overall vulnerability to TF is therefore considered low, in line with the overall risk profile of the jurisdiction as a whole.

7.8 Gambling

Sector Overview

Gibraltar has a small and closely regulated gambling sector consisting mainly of remote gambling operators in the Business to Customer ("B2C") and Business to Business ("B2B") (e.g. game supply) sectors with one casino licence holder operating a land-based casino and two betting premises. Several low-stake, recreational gambling machines are in premises (such as bars and restaurants) throughout Gibraltar.

As can be seen from the figures below, the number of gambling operators has remained steady.

<i>Year</i>	Land-based Casino	Remote B2C Gambling Operators	Betting Shops	Non-casino Gaming Machine Suppliers	Non-casino Gaming Machine Premises
2019	1	17	1	9	106
2020	1	18	1	9	87
2021	1	18	1	9	103
2022	1	20	1	9	102
2023	1	21	1	8	107
2024	1	21	2	7	106
<i>Number of Customers</i>		Approx. 10,000,000 active customers across the sector			

TABLE 29 - MATERIALITY OF GAMBLING SECTOR

The two principal risks within the gambling sector are criminals owning or controlling gambling licences and the services offered by licence holders being used by criminals who spend the proceeds of crime with gambling operators.

The GGC mitigates the risk of gambling operations being run by criminal organisations through its licensing process. All licence applications are assessed, and a range of factors considered to ensure that each licensee is fit and proper. This helps to ensure that criminal elements are unable to own or control gambling operations. The extension of due diligence to critical supplier approvals further mitigates risk. The focus of licensing is to understand the nature of ownership and control including the identification of all ultimate beneficial owners.

As such the residual risk present in all the gambling scenarios in Gibraltar, particularly online gambling, is related primarily to customer-related ML in which proceeds of a crime may be used to gamble (e.g. theft from employer/ proceeds of fraud etc.). Whilst theft and fraud cases are only a very small percentage of the total relative size of active customer numbers, nevertheless the risk of operators accepting deposits from the proceeds of crime is a crystallised risk which is mitigated to a significant extent by effective ongoing customer monitoring and due diligence. Historically operators have had a high risk appetite for large depositing and losing customers. Effectiveness of controls is now a key regulatory focus. While compliance failures have been found these have tended to be isolated rather than systemic and have been dealt with by way of enforcement or remedial action as appropriate and have not in general been found to have involved the actual proceeds of crime.

The Poker vertical is a higher risk area with "chip-dumping" and peer-to-peer transfers of funds between players being a feature on online poker platforms. Lower-level transfers of funds can be effected and this is recognised as a potential ML/TF risk, although collusion in poker rooms can also take place for legitimate non-criminal (gameplay) reasons.

The fact that the gambling sector has been the largest SAR contributor over the last six years is due primarily to its comparatively large non-resident customer base. The predominant predicate offence indicated in these SARs is "proceeds of crime", i.e. the use of self-generated proceeds to place a bet with 90% of the SARs total and 6% indicating ML. There is little in the way of evidence of traditional ML being carried out through online gambling operators.

The gambling sector is not considered attractive for TF or PF purposes.

Remote Gambling (Betting, Casino, Bingo, Poker)

The B2C remote gambling market operates in different but complementary sectors: betting, betting intermediary (exchange), gaming, including slots, bingo and poker, and other products (lottery bets, exchange bets). The majority of B2C licensees provide a full suite of products (fixed odds sports betting, casino products, slot games).

Gibraltar is an international hub for remote gambling operators in both the B2C and B2B sectors and is a major contributor to Gibraltar's Gross Domestic Product (GDP). Gibraltar licensed B2Cs represent approximately 8 million active customers at any given time. The majority of B2C licensees have the UK as their dominant market, and a large proportion of the British remote gambling market is supplied by Gibraltar operators.

When considering the gross gaming yield (GGR) of the different operators, it can be determined that approximately 72% of gambling activity undertaken in respect of Gibraltar licences is UK and Ireland facing activity, with 28% representing rest of the world business. Most business undertaken by Gibraltar operators is therefore with lower risk jurisdictions according to guides such as the Basel AML Index.

Gambling operators are required to be licensed and regulated for their activities, and extensive barriers to entry exist to prevent criminals and their associates from owning or controlling operators. Furthermore, the significant percentage of UK facing activity among licence holders means that all these operators are subject to a dual licensing and regulatory regime with the UK which results in a highly regulated sector where compliance deficiencies are dealt with by way of remedial actions and enforcement where necessary.

Various controls also exist to detect and prevent unlicensed operators from using Gibraltar for unlicensed gambling activities.

The main vulnerability for on-line gambling in the B2C sector arises out of the non-face-to-face interaction between the players and the operator. However, on-line gambling offers significant mitigating features: measures to identify and verify customers (including sanctions and PEP checks) begin with the registration process and all customers are required to have accounts; remote operators use software to enable them to validate a customer's identity and prevent fraud. B2C operators also record and track all customer activity with all transactions being recorded and monitored. The majority of the approximately 10,000,000 active customer base across Gibraltar licence holders are low wagering, low risk individuals. For example, the latest data points to a total of 527 PEPs across all licence holders which represents a very small proportion of the customer base.

While a small number of potential matches to relevant sanctions designation lists have been flagged by operators, these cases have not resulted in any confirmed or material concerns. All operators employ regulatory technology to assist in automated sanctions screening and the Gambling Division assures that these systems are in place and functional during onsite assessments. The lack of positive hits indicates that the regulated remote gambling sector is not an attractive one for sanctioned individuals.

The main threat encountered in remote B2C operations is that of criminals spending the proceeds of crime (including theft from employer cases and the sale of illicit goods) for leisure purposes as opposed to the traditional ML (placement, layering, integration) of criminal funds. The spending of criminal proceeds for the purposes of gambling is therefore the principal risk event that has been found to occur in respect of remote gambling. As well as the potential ability of criminals to be able to spend their illicit gains and the losses this presents to the victims, the potential for this risk materialising also presents a reputational risk to the jurisdiction.

In the B2B sector the principal concern in respect of ML is that where B2B operators (casino games, poker networks and betting data providers) offer their games to B2Cs, no single

operator has full visibility of player data and correspondent gambling activity to allow for the effective identification and investigation of suspicious activity. That said B2Bs can identify suspicious betting patterns and non-standard game play and report to the B2C. B2Bs do not deal with customer funds and therefore their role in the AML/CFT sphere is a tangential one.

Land-based Casinos

Gibraltar has one physical casino.

Ownership and control of casinos by criminals or those associated with crime groups is a risk mitigated by robust due diligence at the licensing stage. The placement of criminal funds as gambling deposits and subsequent withdrawal as winnings (thus legitimising the source of cash) is the other main risk area. The provision of casino facilities in Gibraltar (also including the provision of bingo) is essentially high churn, high footfall leisure activity and the incumbent operator has extensive controls around “high roller” (VIP) activity. Such activity is generally conducted under membership conditions with ongoing monitoring and payment method controls.

There has been a moderate increase in SARs from this sub-sector which evidences an increased understanding of ML/TF risks. The ML risk appears to be well-managed and the nature of the business model may not give rise to significant crystallised risk. Supervision is focussed on the effectiveness of controls and cross-border risk is factored into risk assessment and controls.

Betting (Land-based)

There are currently only two betting shops that operate in Gibraltar which are licensed and regulated by the Gambling Division. These licences were awarded to a longstanding and experienced licensee and the Gambling Division’s supervisory activity has demonstrated that the licensee is complying with its AML/CFT obligations. The licensing process all 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 ML threat.

Three basic ML scenarios can be identified in respect of betting shops:

1. a perpetrator places a bet and cashes in the winnings (conversion);
2. a perpetrator places money in a betting account in one location and an accomplice withdraws the funds in another (e.g. an online channel) (concealment, disguise and transfer);
3. a perpetrator can increase their odds of winning by placing bets on a series of events which will give more favourable accumulated odds (but reducing his chances of winning) or reduce the risk of losing by hedging bets (i.e. betting on both possible outcomes of the same event).

There is some risk in the fact that anonymous customers can place bets. However, the use of CCTV and employee interaction assists the betting shop in building a profile of its customers and can monitor any higher spending customers. The use of cash presents a further risk. The risk of any substantial ML is mitigated by the limits set by the betting shop in respect of how much may be staked over the counter and the nature of the business which comprises low level leisure betting from locals and holiday makers.

Gibraltar has a highly regulated gambling sector covering all aspects of gambling. This regulation mitigates the identified inherent risks considerably. Furthermore, the size and nature of the betting shops in Gibraltar, in respect of the number of customers frequenting it and the level of bets that may be placed substantially limit the risks posed.

Bingo (Land-based)

Offline or land-based bingo is a game of chance, in which the player uses a scorecard, which can be electronic, bearing numbers. Bingo is played by marking or covering numbers identical to numbers drawn by chance, whether manually or electronically. It is won by the player who first marks or covers the 'line' which is achieved when all five numbers on one horizontal row on one scorecard are drawn, or when the player is first to complete the 'house' or 'bingo' when all the numbers on one scorecard are drawn.

Bingo takes place in the licensed land-based casino 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 and they must obtain approval before the event takes place. The risk that bingo operations could be co-opted by criminals to launder criminally derived funds is therefore substantially mitigated. Bingo in Gibraltar is not a large-scale activity and therefore the corresponding risk is a lower one. The use of CCTV and effective monitoring activity within the casino premises also mitigate the risk that individuals could launder or spend the proceeds of crime in the bingo hall.

There is negligible risk of ML/TF in this area in Gibraltar.

Lotteries (Gibraltar Government Lottery)

The relatively low return to players makes direct purchase of lottery tickets a costly and unattractive form of ML. On the contrary, the modus operandi of purchasing a winning ticket - a perpetrator purchases a lottery ticket from the winner and cashes the prize with a receipt, is more viable scenario reported by LEAs.

Gibraltar only operates one state run Lottery and the risk of ML through the purchase of winning tickets is considered low due to the relative low pay-outs of the lottery and the uncertainty inherent in such an approach, making this unattractive for large-scale ML schemes.

Poker (Offline)

Poker is organised in licensed premises (such as the casinos). It is either organised as a tournament, where a poker player enters by paying a fixed buy-in at the start and is given a certain number of poker chips (the winner of the tournament is usually the person who wins every poker chip in the tournament) or as a table game where the player can buy more poker chips as the game continues. Unlike many other gambling products, participants play against each other and not against the organiser of the activity. The organiser will receive a fixed amount of the turnover (a rake) or winnings.

The ML risk scenario is that a perpetrator purchases chips at the casino (for cash or anonymous pre-paid cards) and these chips may be transferred to another player through deliberate losses (folding on a winning hand to ensure that the accomplice receive the chips known as 'chip dumping'). Chips are converted into cash or transferred in another way to the customer.

This channel is perceived as rather attractive although it requires moderate levels of planning (complicity) or technical expertise (gambling strategy itself) to make use of illicit tournaments or to deliberately lose so that an accomplice can win.

Poker events take place at the licensed casinos and the Gambling Division is informed beforehand of the arrangements to ensure that the poker events are adequately supervised using effective CCTV positioning and supervision on the part of employees. 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.

The land-based casino has undergone a stringent licensing process to ensure its suitability and is regulated by the Gambling Division.

Gaming Machines (non-casino)

Gaming machines (offline) based on a random number generator are normally divided into several subcategories, depending on the maximum stake, maximum winnings or the type of premises the gaming machine can be placed in.

While the anonymity of customers using gaming machines presents a potential enabling factor for laundering the proceeds of crime through gaming machines there is little evidence of this vulnerability being exploited. Furthermore, gaming machines do not appear as an attractive option for ML due to the inherent chance element, low stakes and winnings combined with the time and effort required to launder any significant amounts of money.

Threat and Vulnerability Assessment

The ML/TF risk within the gambling sector can be attributed primarily to two concerns. In respect of ML the risks lie both in the potential criminal ownership and control of gambling operators and in the potential use of gambling services offered by said operators being used as conduits for the laundering or mere spend of the proceeds of crime.

The foremost means in which ML activity takes place within the gambling sector is through the simple spending of the proceeds of crime for leisure purposes by lifestyle criminals, or due to an association with problematic gambling (theft from employer or breach of position of trust), rather than the traditional laundering of funds *per se*. Whilst an operator's own risk management and fraud controls may substantially reduce the opportunity for traditional ML to take place, departures from best practice and failure to follow internal policy and process still create residual risk and the opportunity for criminal exploitation. For example, allowing significant and sustained wagering on low odds favourites without requisite and proportionate levels of CDD.

Case Study

In one case, several operators received monies that had been stolen from an employer by an individual in a position of trust who had fraudulently forged documents and provided false information in relation to evidencing his wealth and source of funds. This was identified due to intelligence received from the GFU that several operators had submitted a suspicious activity report in respect of the same individual. This led to a review by the Gambling Division into operator systems and controls where it was found that appropriate EDD had not always been conducted on high depositing customers irrespective of whether they were also losing large amounts. There was also the divestment of any profit by the operators, as well as a regulatory settlement in lieu of a financial penalty.

The TF threat is not considered to be of significant likelihood although the impact would be severe. Intelligence provided to the relevant authority and information obtained during its supervisory activities do not lead us to believe that the TF threat has materialised although there are certain products that could lend themselves to the potential passing of funds destined for terrorist activities between one customer and another. In this respect the primary risk has been determined to be that of poker and the possibility of peer-to-peer transfers between users of the poker platform. This can occur either as transfers involved in 'staking' players or through the deliberate losing of funds (so-called "chip dumping") by one player to another. The inter-account transfers between players have historically been considered to be a particular area of vulnerability due to the risk appetite of players, operational staff and affiliates in the poker sector and the fact that historically this has not

been an area where every operator has had proportionate controls over such transfers; this is no longer the case due to operators closing down this function.

The other potential TF issue lies in a sanctioned individual utilising the services of a gambling operator.

Similarly, the risk of the gambling sector being utilised for the purposes of financing the proliferation of weapons of mass destruction is considered low although the impact if it was to happen would be severe. Licence Holders should therefore remain mindful of the need to monitor unusual activity and transactions, in respect of any peer-to-peer transfers and to maintain effective screening programmes in relation to their customer base. This is particularly the case in respect of indirect financing which could contribute to the proliferation of chemical, biological, radiological and nuclear weapons, using peer-to-peer gambling services.

The B2B sector does not fall under the provisions of the POCA regime due to not dealing directly with customer funds. Nevertheless, it remains an important factor in assisting in keeping financial crime out of the gambling sector due to B2B operators' ability to monitor customer gameplay for any potential red flags and alert the relevant B2Cs where necessary.

7.9 Insurance Sector

The insurance sector in Gibraltar consists primarily of general insurance companies and is one of the largest contributors to the local economy.

General Insurers	General Insurance Intermediaries	Life Assurers	Life Assurance Intermediaries
37	23	3	13

TABLE 30 - MATERIALITY OF INSURANCE SECTOR AS AT 31 DEC 2024

To note that from the 3 life assurance companies, 3 form part of the same Group.

There are a number of insurance intermediaries who are authorised to carry out life insurance intermediary services, however, only 2 of these are actively doing so. The remaining 7 firms are only carrying out general insurance intermediary services and so, are also caught in the number for General Insurance Intermediaries.

The majority of these firms underwrite risks outside of Gibraltar. Gibraltar's insurance industry is estimated to underwrite approximately 30% of all UK car insurance policies.

In contrast, the provision of life assurance products is relatively small and is undertaken by only a handful of local insurers who issue policies in lower risk jurisdictions.

Composition and size of the Financial Sector -Life and other Investment Linked Insurance	
Number of insurance companies that offer life insurance and other investment linked insurance	18
have branches and subsidiaries abroad	0
Total Premium Income	£37,898,524
Total number of clients	35,369

TABLE 31 - COMPOSITION AND SIZE OF THE LIFE AND OTHER INVESTMENT LINKED INSURANCE AS AT 31 DEC 2024

SARs submitted by this sector share similarities with the other sectors examined in that fraud, proceeds of crime, ML and tax crimes are the most common occurrences for knowledge or suspicion.

General Insurance

As detailed above, the insurance sector in Gibraltar is predominantly driven by general insurance, which is considered to pose a low risk of ML/TF.

Non-life insurance policies are typically short-term in nature and serve to provide protection against unexpected loss, such as damage to property. Based on the gross written premiums, the most dominant lines of non-life insurance business are those linked to motor vehicle liability, fire and other forms of damage to property, as well as medical expenses. In Gibraltar, motor vehicle liability insurance plays a dominant role in the general insurance market.

ML can occur in the context of insurance fraud involving non-life insurance, where individuals attempt to recover illegitimate funds through claims. These scenarios are often characterised by frequent premium payments and cancellations. The risks may arise or materialise where an insurer:

1. Accepts premium payments in cash, although this is not a common practice; or
2. Refunds premiums, upon policy cancellation or surrender, to an account other than the source of original funding (owned by a party other than the policyholder).

Point 1 could facilitate ML by initial placement, whereas point 2 could be used for layering and integration. Neither of these points have been identified as trends locally.

Similarly, there is a potential risk of TF associated with insurance fraud, as it could serve as a source of funding for terrorist activities. However, this method typically involves extensive planning and large paper trails, which may deter terrorist groups from pursuing it.

The risks of these activities occurring in Gibraltar are mitigated primarily through the legislative requirements and supervisory regimes that these firms are required to adhere to. The majority of general insurers in Gibraltar are also managed and administered by authorised insurance managers. These firms provide an additional layer of oversight and assessment over the controls employed by the insurance company as well as providing day-to-day management and administrative support. Insurance managers are caught by POCA 2015 and therefore are required to comply with all AML/CFT obligations.

Life Assurance business

As stated above, the Gibraltar life assurance sector is composed of 3 entities, 2 of which form part of the same group of companies. Life assurance companies offer a range of investment products, with or without guarantees, incorporating life assurance benefits.

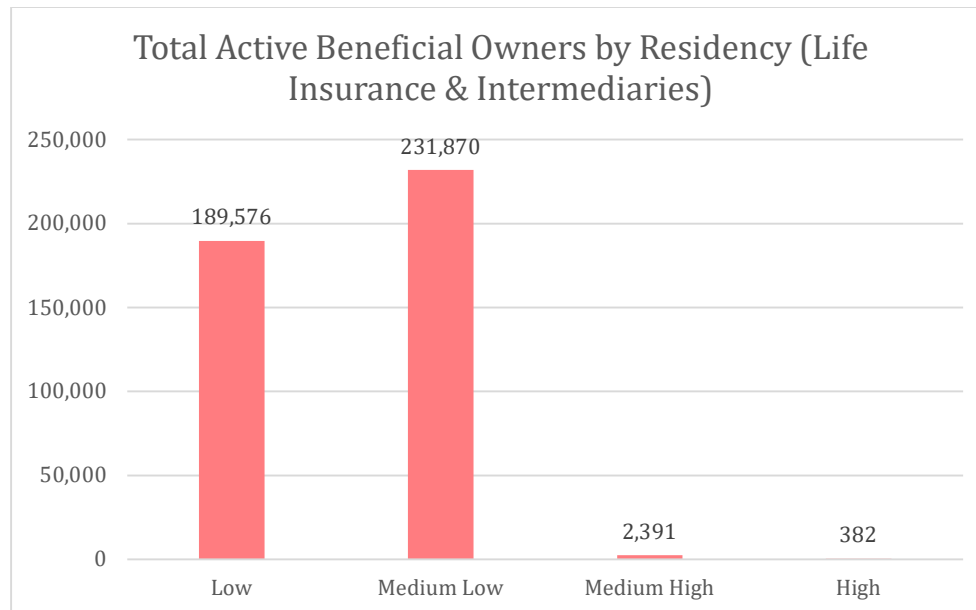


FIGURE 15 - PROPORTION OF CUSTOMERS ATTRIBUTED TO LOW VERSUS HIGH RISK JURISDICTIONS IN 2024

ML/TF risks in the insurance industry primarily relate to life assurance and annuity products. These products allow potential customers to inject funds into the financial system, potentially disguising their criminal origin or to finance illegal activities. Relevant risk scenarios typically involve investment products rather than death benefit products.

ML Threat and Vulnerability

The potential ML risks may arise where:

1. An insurer accepts a premium payment in cash;
2. An insurer refunds premiums, upon policy cancellation or surrender, to an account other than the source of the original funding (owned by a party other than the policyholder);
3. An insurer does not carry out adequate CDD or establishes the source of investments (no instances of this have been identified locally);
4. An insurer sells transferable policies (these are uncommon);
5. Investment transactions involve trusts, mandate holders, etc;
6. An insurer sells tailor-made products, where the investor dictates the underlying investment or portfolio composition; and/or
7. An insurer sells a small investment policy initially and the investor makes subsequent large investments without undergoing additional CDD (no instances of this have been identified locally).

The GFSC's Annual Financial Crime Return data demonstrates that there are no notable threats regarding the above typologies. The points listed above are either extremely uncommon in Gibraltar or are disallowed under local legislation (such as the requirement for all firms to conduct CDD). Additionally, the assessment of these potential risks would occur both prior to the point of authorisation as well as part of the ongoing supervision of the regulated entity by the GFSC. This would therefore ensure that Gibraltar's life assurance firms are further limiting their exposure to ML risks. Therefore, the risk is considered low.

TF Threat and Vulnerability

TF threat related to life insurance generally in all jurisdictions shows that terrorist groups have limited interest in this method. Usage of these means would require a high level of specific knowledge on the product and its characteristics. Additionally, life assurance contracts are not easily accessible, and applications require a lot of supporting documentation, which is likely to dissuade terrorist groups. Foreign terrorist fighters may theoretically also attempt to take out life assurance with the request that the funds be redeemed for the benefit of their family in the event of their suicide or death. However, legislation or insurance companies' underwriting policies often do not allow for such a clause, greatly lessening the risk of this occurring. Data from the GFSC's Annual Financial Crime Return shows that only 0.04% of customers are resident in conflict zones.

In conclusion, the small number of authorised life assurance firms in Gibraltar, combined with low premium levels and exposure associated with these firms lessens the potential risk that they pose to the jurisdiction. This is further mitigated by the GFSC's authorisation and regulatory regime in assessing these controls. Therefore, the risk is considered low.

7.10 Real Estate

Materiality

Composition and size of the Real Estate Sector	
Total number of real estate agents, of which:	29
Sole practitioners	6
Real estate brokerage firms, of which belong to international groups or networks	3
Number of real estate deals	344
Total value of real estate deals	£202,179,577
Total number of clients	2,775

TABLE 32 - MATERIALITY OF THE REAL ESTATE SECTOR AS AT 31 DEC 2024

Description of Sector

Gibraltar is a very small territory covering an area of approximately 6.8 km. Of this area approximately 40% consists of the upper rock nature reserve that is a mostly uninhabited protected area. As at 31 December 2024 there are approximately 19,200 properties in Gibraltar. Of these 3,900 are commercial that are traditionally held on shorter lease terms. Of the remaining 15,300 properties there are four types of residential properties:

1. Government of Gibraltar (GoG) rental stock: 100% owned by GoG, let directly by GoG's Housing Department to Gibraltarians and cannot be sublet (approximately 5,300 properties at subsidised rents <£200 per month);
2. Co-ownership properties: Government funded "affordable" properties, subject to a minimum 3 year Gibraltar residency requirement, often co-owned between GoG and the occupier and with rental restrictions (approximately 4,900 properties). These properties are sold to residents who are on waiting lists and generally, who have not previously owned property. These properties are sold directly by GoG who do not charge a premium for the land or a profit on the construction;
3. Open market properties: not generally subject to restrictions, are available to any owner or occupant and can be rented (approximately 4,800); and

4. Ministry of Defence properties: exclusively available for occupation by the British Forces personal (approximately 300).

The value of an open market property is approximately double the value of an equivalent co-ownership property reflecting the restrictions imposed on the latter. In 2025, the average value of open market properties is £603,765, off-plan properties is £562,935, and those with three year restrictions is £403,479 which are within expected ranges. Significant fluctuations in property values could potentially indicate speculative activities associated with ML, but the consistency here suggests a more stable market.

Due to Gibraltar's small size, there are limited opportunities for property development in new areas of Gibraltar. A large proportion of properties are located on land reclaimed from the sea due to limited space for development. While there is a boom in construction to try to meet the demand for new properties, newest developments are on land previously used for non-residential purposes or renovations of pre-existing buildings. New reclamation projects have been announced by GoG to alleviate this demand. It is normal for off-plan properties to be sold-out and resold prior to completion.

The scarcity of land keeps demand and property prices generally high. Only open market and commercial properties however are considered to be suitable for investment and therefore it is expected that criminal groups would only target these categories of properties. This only represents 25% of the residential property market of which the majority are occupied by locals and foreign workers and expats in Gibraltar who are not eligible for co-ownership properties. Local criminals eligible for co-ownership properties may however see these attractive although the exchange of funds in such circumstances would be limited and for a single transaction only as eligibility is for one co-ownership property only.

The open market property rental market is attractive for investment due to the big demand for rental accommodation as there is limited rental stock and there are tax consequences for any person who works in Gibraltar but resides in Spain. The opportunities for criminal groups seeking to launder funds on a significant scale however are similarly reduced by lack of availability of properties. This is also further reduced by the increase in compliance standards that are presently applied by the Real Estate Sector. The letting of other properties is not deemed attractive for international criminals due to the restrictions on rentals. There may be limited attraction of GoG rental stock and non-declared rental of restricted co-ownership properties to low level local criminals if they are seeking to rent homes for their own use, however the exchange of funds in such circumstances would be very small.

Real Estate Agents (REAs)

Real estate agents (REAs) include businesses which provide services associated with the buying, selling and leasing of property as defined in POCA. They are subject to AML/CFT requirements and are licensed and regulated by the Office of Fair Trading (OFT). REAs are required to carry out CDD on both parties to a real estate transaction before proceeding with the same. The effectiveness of the OFT's onsite inspections demonstrates the sector's commitment to compliance. Findings from initial onsite visits in 2022 compared to visits in 2024 reveal significant improvement in the sector:

- Breaches fell by 75.38%
- Deficiencies fell by 69.09%
- Action plans fell by 50%
- Action plan recommendations fell by 71.63%

Unlike REAs in other jurisdictions, Gibraltar REAs only receive a commission on the transfer of real estate, which is usually between 1 and 2% of the purchase price, but do not handle the remaining 98% of the purchase funds which are instead handled in their entirety by lawyers, who are also regulated for AML/CFT, through their client accounts. This substantially

decreases the attractiveness to criminals using Gibraltar REAs for laundering and therefore reducing the ML/TF threat as money would not flow through them. From the data collected from the annual returns submitted for 2024 the total commission earned, £3,001,736, accounted for approximately 0.06% of the total property sales value, £5,402,384,455. A higher commission percentage might indicate potential irregularities or excessive financial flows, but the relatively modest commission suggests a standard and transparent fee structure.

The majority of transactions (96.5%) are conducted through bank transfers (banking sector is also heavily regulated for AML/CFT) or card payments, which are traceable and leave an audit trail. There were no payments made in cryptocurrency. This transparency in payment methods reduces the likelihood of illicit funds flowing through the real estate sector unnoticed.

Only 3.5% of transactions involve cash. Cash transactions are often associated with higher ML risks due to their anonymity. The low percentage here suggests a reduced potential for illicit activities, as most transactions are conducted through more traceable means. The low volume of cash transactions also means that there is a reduced risk of tax evasion, fraud, corruption as well as a shift towards a safer, more secure technological method of payment that promotes overall systemic security. The level of payments received from higher risk countries is negligible, 0.1 %, and there is nothing to suggest that terrorist financing is occurring within the sector to date. 74.75% of payments originate from Gibraltar, 23.97% from UK and 0.71% from EU countries and 0.57% from the rest of the world.

There are 29 REAs in Gibraltar, some also offer their services for properties in other jurisdictions, most notably in Spain. The breakdown of customers shows a diverse base with 47% Gibraltar nationals, 40% UK nationals, 11% EU nationals and 2% other nationalities.

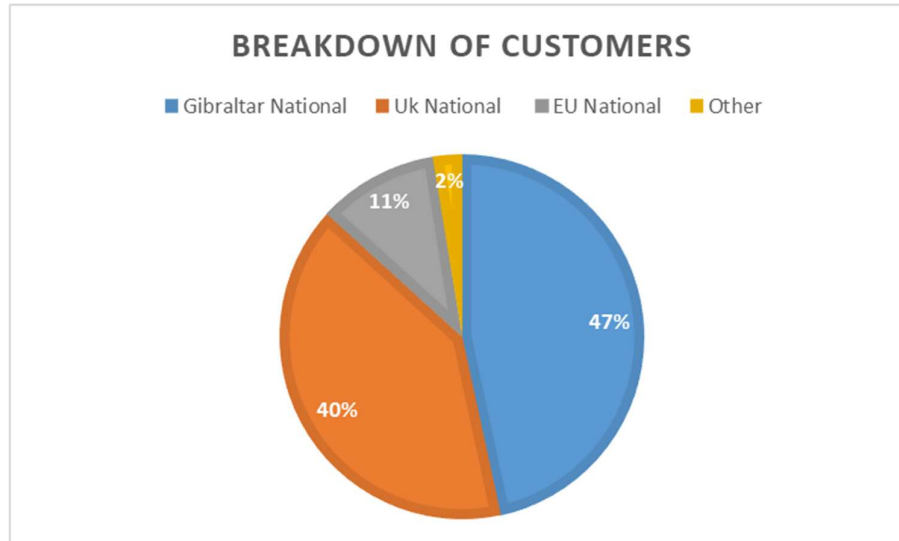


FIGURE 16 - REAL ESTATE CUSTOMER BREAKDOWN AS AT 31 DECEMBER 2024

Of the customers who bought residential properties, 77% were bought properties as homes (owner occupiers), and only 23% bought properties for rental or speculation. The involvement with PEPs is relatively low, with 59 (93.65%) (PEPs being local PEPs and only 4 (6.35%) international PEPs. PEPs are considered higher risk due to their potential influence and access to public funds. As Gibraltar is a very small jurisdiction it is very easy for the sector to identify PEPs and thus conduct enhanced CDD for these individuals.

All real estate transactions involve in-person interactions. Face-to-face transactions generally provide a higher level of scrutiny and reduce the risk of fraudulent activities associated with remote transactions, 98% of transactions were carried out face to face and only 2% of transactions were carried out none face to face, lowering the risk of corruption.

The OFT has implemented a robust supervisory framework that includes the issuance of detailed guidance notes, specifically on CDD requirements, and has an ongoing schedule for on sites, and so far has carried out an onsite inspection on every REA at least once as part of its ongoing schedule of onsite supervisory assessments. These measures have significantly reduced the ML/TF vulnerability of this sector. Additionally, all licensed REAs are required to carry out an annual risk assessment of its business, submit an annual report to the OFT and to implement internal control systems to identify, assess, and mitigate ML/TF risks. to

7.11 High Value Dealers

The Office of Fair Trading (OFT) in Gibraltar is responsible for regulating goods dealers and ensuring compliance with AML/CFT obligations under POCA. High value goods dealers (HVGDs) are subject to AML/CFT requirements when conducting cash transactions exceeding the monetary GBP equivalent of EUR 10,000.

Currently, there are no HVGDs in Gibraltar that have a cash policy whereby they accept more than the GBP equivalent of EUR 10,000. This contributes significantly to the low vulnerability of the jurisdiction to ML/TF risks. Gibraltar's unique retail market, characterized by the limited number of businesses, particularly those handling high-end luxury items, combined with the small retail market and no inclination toward large cash transactions, reinforces the overall low risk of ML/TF in this sector.

Notwithstanding the absence of HVGDs in Gibraltar that accept more than the GBP equivalent of EUR 10,000, the OFT engages with goods dealers generally, and in particular those handling high-value items that are paid for by non-cash methods. It is this engagement that led to the implementation of no cash policies restricting the acceptance of payments exceeding the monetary GBP equivalent of EUR 10,000 in cash. Furthermore, the majority of businesses in Gibraltar prefer non-cash transactions due to local bank-imposed cash deposit fees, resulting in a reduced likelihood of large cash transactions.

The collaborative effort between the OFT's AML section and the Business Licensing section of the OFT further strengthens the regulatory framework. Through joint initiatives, these sections carry out comprehensive initial and ongoing due diligence, including sanctions checks, on licensees. The proactive nature of these checks allows the OFT to identify and address potential risks promptly. In conclusion, the combination of targeted regulations, proactive engagement, limited cash transactions, and effective collaboration between OFT sections positions HVGDs in Gibraltar as low-risk entities for ML/TF activities. Artefacts, Art and Antiquities

Arts dealers are inherently considered high risk dealers as the international trafficking of looted artefacts and antiquities is internationally recognised as one of the biggest criminal trade categories. The OFT has therefore created additional record keeping requirements applicable to these dealers in Gibraltar as set out in the OFT's AML/CFT Guidance Notes for HVGDs.

The market for the sale of artefacts, art and antiquities in Gibraltar is very small however with only 7 licensed art and antique dealers in the jurisdiction selling low value items. All have been engaged by the OFT who have carried out onsite visits. The OFT has engaged with these businesses to raise awareness and to ensure compliance. There are also currently 2 art market participants as defined by POCA. The ML/TF threat is therefore considered to be low.

Precious Metals and Stones

It is internationally recognised that criminals favour precious metals such as gold and stones such as diamonds as they are inexpensive to store and easy to turn into cash. The purchase of gold and diamonds is easily accessible and requires moderate level of planning and expertise. Gold is also commonly used in war zones and is therefore viable and attractive for terrorist groups.

For these reasons dealers in precious metals and stones are considered by the OFT as posing a higher risk than dealers in other goods. It has therefore increased the record keeping requirements applicable to these dealers as set out in the OFT's AML/CFT/CPF Guidance Notes for HVGs. Dealers are licensed and regulated by the OFT and are subject to onsite inspections. The OFT has encouraged these dealers to implement policies not to accept payments above the monetary GBP equivalent of EUR 10,000. 100% of jewellers have introduced such policies.

In Gibraltar there is no wholesale market for the exchange of diamonds and bullion. The only market for precious metals and stones is through local jewellers in small retail quantities and mostly of low value. The biggest ML/TF threat is considered to be the direct purchase by local criminals of jewellery and timepieces for their own personal use and consumption. Another vulnerability is the purchase by Gibraltar jewellers, inadvertently or otherwise, of gold and jewellery which has been bought with illicit funds in another jurisdiction through a broker using false invoices and certificates.

Gibraltar's number of dealers in precious metals and stones is small and comprised of jewellery retailers who mainly carry out face to face transactions with domestic or Spanish customers. As at 31 December 2024, there are only 34 licensed jewellers trading within Gibraltar, many of which are part of three main jeweller groups owned by the same beneficial owners and which trade mainly in jewellery and timepieces as opposed to precious metals by weight, bullion and loose diamonds.

Cars and Marine Craft

Certain high value goods such as motor vehicles and boats are particularly attractive to criminals as both lifestyle goods and economic assets. Criminal cash can be converted into goods that are in high demand in foreign markets. While all of these items may be purchased in Gibraltar the dealers in these goods are few and easily identifiable.

There are only five licensed marine craft dealers in Gibraltar. None have a substantial showroom however and most sell these goods to order, sometimes via brokers. While this could elevate their ML/TF exposure, as they could be more attractive to criminals wishing to import new marine craft, the five dealers have very limited activity and import on a retail basis only. All have been engaged by the OFT, have implemented AML/CFT policies, have implemented cash policies below the monetary GBP equivalent of EUR 10,000 and report annually to the OFT.

Due to the small scale of trading in Gibraltar the risk of these high value goods being used for ML/TF schemes is mitigated considerably as not many opportunities are presented to criminals other than the purchase of these lifestyle goods for their own use.

There are 16 licensed car dealers in Gibraltar that mainly supply the local population. Given the limited market most dealers generally have exclusivity in the jurisdiction over specific marques that they sell through bespoke show rooms. It is therefore very easy to identify cars sold by particular dealers unless they are sold second hand which increases the businesses exposure should they not fulfil their AML/CFT obligations. The OFT has also encouraged these dealers to implement policies not to accept payments above the monetary GBP

equivalent of EUR 10,000 with 100% reporting they had implemented such policies and not accepted any cash in the last reporting period.

The assessment of the TF vulnerability related to the purchase of other kinds of high value goods (other than gold, diamonds, artefacts and antiques) is not considered relevant.

Threat and Vulnerability Assessment

The OFT licences all goods dealers in Gibraltar to carry on business. These business licences are relied upon by HM Customs to assess the legitimacy of the importation for the relevant goods into the jurisdiction. The POCA imposes AML/CFT obligations on HVGs where they sell high value goods in cash. The OFT has also successfully encouraged dealers to implement cash policies not to accept cash above the monetary GBP equivalent of EUR 10,000.

7.12 Legal Professionals

The legal sector is regulated by the Legal Services Regulatory Authority (LSRA).

7.13 Composition and materiality

Gibraltar has a well-developed, mature and stable legal sector. As of 31 December 2024 it was composed of:

- 42 private legal practices (comprising the individuals in 2 below), of which:
 - 21 are law firms, almost all of which are well-established and can trace their establishment back decades; and
 - 21 are sole practices;
- 343 legal professionals (as defined in the Legal Services Act 2017) are registered with the LSRA as Authorised Persons to provide various types of legal services in or from Gibraltar, of which:
 - 287 Legal Professionals work in private practices and may carry out relevant financial business (RFB) as defined in POCA;
 - approximately 240 Legal Professionals practise as part of law firms; and
 - approximately 150 Legal Professionals practise in the four largest law firms, of which one is considered very large.

Legal Professionals carrying out RFB are supported by other administrative staff (67 in all practices), who assist with gathering CDD, handling client monies and preparing client or matter risk assessments.

Composition and materiality of the Legal Sector	Number
Total number of legal practices, of which:	42
Law Firms	21
Sole practitioners	21
Practices undertaking Relevant Financial Business ('RFB')	29
Number of Relevant Financial Business (RFB) transactions	2,829
Monies paid into client accounts re RFB transactions	£668m
Number of RFB transactions for Gibraltar-resident clients	1,066

Number of RFB transactions for non-resident clients	162
---	-----

TABLE 33 - MATERIALITY OF THE LEGAL PROFESSION AS AT 31 DEC 2024

Trust and corporate services activities are not legal services and legal professionals cannot therefore conduct these activities unless they, or the regulated TCSP that they may work for, are separately licensed and regulated by the GFSC (please refer to Section 6.2).

7.14 Types of Relevant Financial Business

While 69% of legal practices undertook RFB, on average this only represents less than 22% of legal practices' overall business. This translates to:

- fewer than 2,900 transactions; and
- £672million paid into legal practices' client accounts.

Of all RFB transactions undertaken by Legal Professionals, over 80% involved the buying and selling of real property. By comparison, the next most significant types of RFB transactions (acting on behalf of and for clients in financial transactions and corporate support services⁷), each represent only around 10% of the volume of RFB transactions undertaken by Legal Professionals.

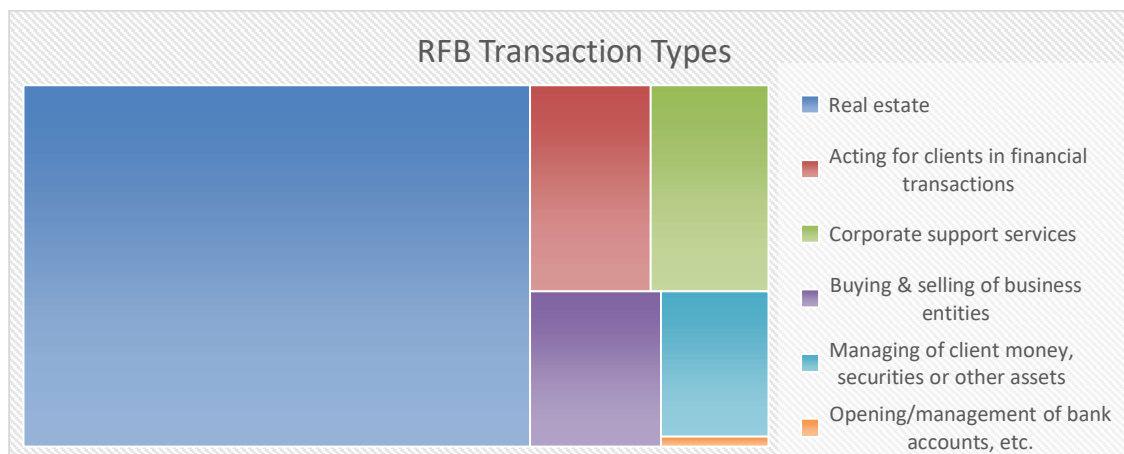


FIGURE 17 - TYPE OF RFB TRANSACTIONS IN THE LEGAL PROFESSION AS AT 31 DEC 2024

Transactions that form part of complex structures only represent 2% of all RFB transactions, indicating a reduced ML/TF risk to the sector in this regard.

Real Estate RFB Transactions

Representing over 80% of all RFB transactions carried out by Legal Professionals, Real Estate RFB Transactions are considered to have the highest ML/TF material risk to the legal sector.

Residential Real Estate RFB Transactions

Of these transactions, those that relate to residential property are the most common (75% by total value of real estate transactions, 94% by number of real estate transactions and 93% by monies received in client accounts).

⁷ Subsections 9(1)(k)(i)(D) & (E) of POCA are represented here in the chart as "corporate support services". Subsection (D) refers organisations of contributions necessary for the creation, operation or management of companies. Subsection (E) refers to the creation, operation or management of trusts, companies, foundations, or similar structures.

The purpose of most residential Real Estate RFB Transactions was the buying or selling by owner-occupiers of their properties (52%). Most transactions therefore involved individuals (or Gibraltar companies with simple shareholding structures) buying property for personal use. This represents a low ML/TF risk as it indicates legitimate reasons for the transactions, with a reduced incentive for criminals to use their own properties for illicit purposes. The transactions are therefore more straightforward and transparent. This is particularly so in relation to the sale and purchase of properties that are subject to Government resale restrictions, representing 23.5% of owner-occupier RFB transactions, as the sale restrictions do not make these properties attractive for ML/TF.

Commercial Real Estate RFB Transactions

In relation to Real Estate RFB Transactions relating to commercial property, the data reflect that most commercial property transactions are for the client businesses' own use (51%). This presents a lower risk when compared to commercial property acquired for other purposes, since the property would be occupied by that business as opposed to a third party with a reduced incentive for criminals to use their own properties for illicit purposes, unless of course the business was set up as part of a ML/TF scheme.

Real Estate RFB Transaction risks

Real Estate RFB Transactions relating to investment or speculative purchases (12% for residential and 17% for commercial), and to a lesser extent off-plan purchases directly from developers (18% for residential and 3% for commercial), present moderate-to-high ML/TF risks because:

- investment or speculative purchases may be geared toward generating quick profits, making them more attractive for money laundering schemes;
- there are greater ML layering opportunities with the potential for regular buying and selling of properties;
- initial deposits may be less transparent when buying directly from developers, and
- the potential use of complex ownership structures that can mask beneficial ownership and conceal illicit funds.

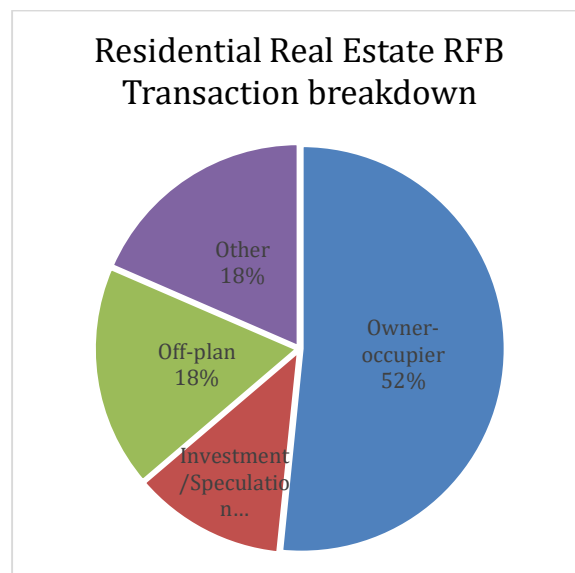


FIGURE 18 - RESIDENTIAL REAL ESTATE RFB AS AT 31 DEC 2024

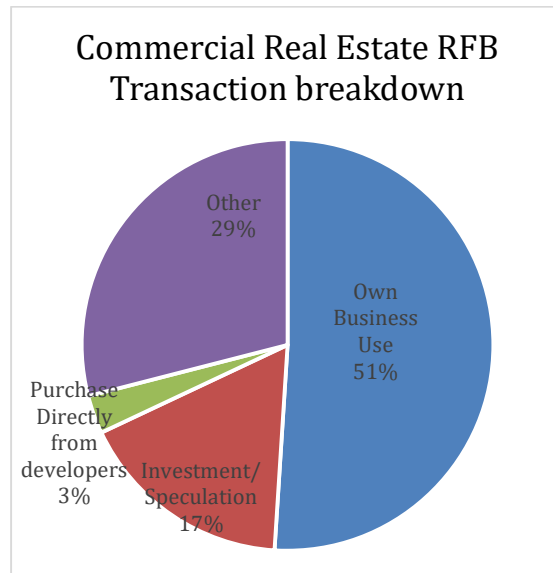


FIGURE 19 - COMMERCIAL REAL ESTATE RFB AS AT 31 DEC 2024

"Other" real estate RFB transactions include matters such as lease extensions, mortgage redemptions and related transactions. These are perceived to have a low ML/TF risk.

Transactions conducted on behalf of and for clients in real estate

31% of the 463 transactions conducted by Legal Professionals on behalf of and for clients relate to real estate. The majority involved legal professionals assisting in the planning or execution of transactions for their client.

The largest ML/TF risk in this regard is that of Legal Professionals becoming an intermediary in ML schemes by directly handling illicit funds. Assisting in planning or executing these activities can also make Legal Professionals more susceptible to being complicit in a client's fraudulent or illegal intentions. The ML risk for this type of transaction is considered moderate, however the materiality of these types of transactions is low with <£12.5 million paid into legal practices' client accounts.

7.15 RFB transaction clients

Despite some larger law firms having an international profile, the data demonstrates that the vast majority of Legal Professionals' RFB clients are Gibraltar nationals (85%), indicating that international clients represent a minority of the sector's client base.

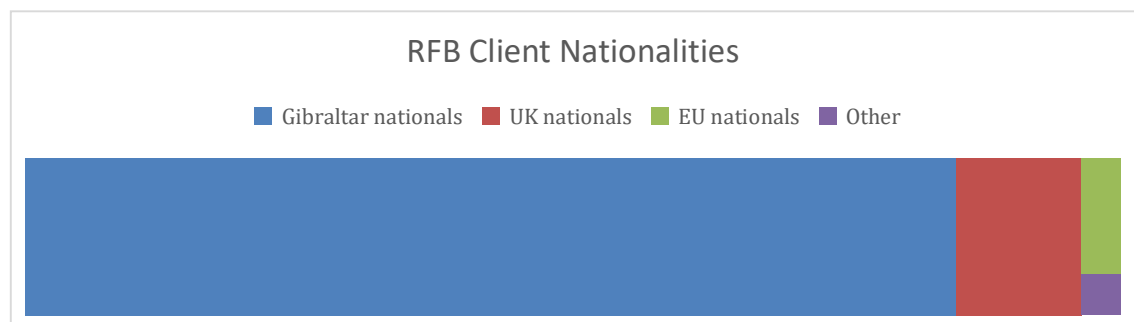


FIGURE 20 - NATIONALITIES OF THE LEGAL PROFESSION CLIENTS IN 2024

Gibraltar clients

The very large percentages of Gibraltar clients, meaning Gibraltar nationals or Gibraltar residents, represents a reduced ML/TF risk given that:

- verifying the identity and background of local or resident clients is generally easier due to access to local knowledge, public records, and familiarity with local legal and cultural norms, particularly in a small jurisdiction like Gibraltar; and
- this indicates a reduced exposure to jurisdictions with varying regulatory frameworks or higher risks of ML/TF, or sanctions evasion.

International clients

Of those international RFB clients, UK (11.4%) and EU (2.65%) nationals represent the vast majority of foreign clients' provenance and these jurisdictions are generally considered lower risk. The number of clients from other countries is very low. At onboarding, very few clients from countries designated by the FATF as a Jurisdiction under Increased Monitoring were identified (0.4%). This reflects a low ML/TF exposure to the sector to clients from higher risk jurisdictions.

RFB transaction clients

77% of the sector's RFB transaction clientele are natural persons. Legal Professionals should nevertheless be wary of clients representing undisclosed third parties, however this risk is reduced by applying CDD obligations as required by POCA.

23% of transactions involve corporate or other entities and/or legal arrangements, each of which requires Legal Professionals to identify the ultimate beneficial owner thereof. At 23%, these clients represent a notable share of RFB transaction clientele for the sector and therefore an elevated ML/TF risk. The main risks are the potential for opacity in ownership and control of these clients, their use of complex structures, and their involvement in jurisdictions with weaker transparency. These entities can obscure the true beneficial ownership, allowing for the layering of funds and the mixing of illicit and legitimate money. Additionally, Legal Professionals must also take into account that non-natural clients may often engage in larger, more complex transactions, which can mask suspicious patterns.

Identified client risk

In terms of client risk, legal practices:

1. considered only 4% of RFB clients to be high risk, as a result of which enhanced due diligence measures were applied (excluding PEPs); and
2. provided legal services to 28 domestic PEPs and eight foreign PEPs.

The low number of identified high-risk clients is encouraging, suggesting that the client base may generally pose a lower risk for ML/TF.

Politically Exposed Persons (PEPs)

Over two thirds of the 28 PEPs serviced by legal professionals were domestic PEPs. Domestic PEPs are generally considered to present a lower ML/TF risk compared to foreign PEPs, of which there were only eight. The level of exposure of domestic PEPs is considered lower as it is easier to carry out CDD checks on domestic PEPs as information is more accessible and there is familiarity with them in such a small community. For this reason, Legal Professionals may be more aware of the risks that may arise if a domestic PEP holds significant influence over financial resources, such as public procurement or funding allocations, or if there are specific corruption concerns in Gibraltar.

Interface Risk

The vast majority of RFB clients were met in person by legal professionals, with fewer than 7% of RFB transactions being non-face to face transactions. This represents a low interface risk across the legal sector.

RFB transaction payments

Payment types

Bank transfers (95%) are by far the most used payment type within the legal sector, followed by a small amount of card or cheque payments. In their most recent regulatory returns, legal practices did not report receiving any payment of fees or client monies in cash and no payments were made in crypto currency or other forms of payment. This represents a lower risk of legal services being exploited for illicit purposes and allows for establishing audit trails through the banking system should any transactions need to be investigated.

Payment Sources

Most payments received by Legal Professionals were from Gibraltar (82%), with 15% being from the UK and only >2% from the EU or other countries. This data correlates with the mainly local client base and with Gibraltar-focussed nature of RFB transactions. Transactions from local banks make it easier for Legal Professionals to conduct CDD, verify client information and identify suspicious activity. Additionally, local payments are less likely to involve complex cross-border structures, offshore entities, or jurisdictions with weaker AML/CFT controls, reducing the opportunity for obscuring the source or destination of funds.

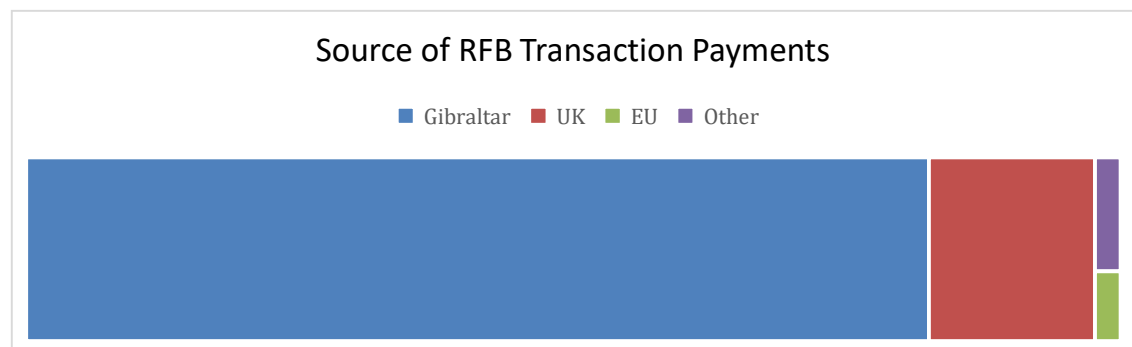


FIGURE 21 - SOURCE OF RFB TRANSACTION PAYMENTS IN 2024

The ML/TF risk with regard to payment sources is also lowered given that Gibraltar, United Kingdom and European Union banks are subject to robust AML/CFT standards.

Other ML/TF risks

Legal services can be misused to launder proceeds from various predicate offences, including fraud and illicit trafficking. ML and fraud are the most common form of offences on which co-operation from Gibraltar is sought, indicating that this jurisdiction's products and services, including legal services, may be targeted to launder the proceeds deriving from predicate offences, even though these underlying offences were not committed in Gibraltar.

Misuse of client accounts.

While there is no evidence of Gibraltarian legal practices' client accounts having been abused for ML/TF, this is considered an inherent ML/TF risk to the sector.

Lawyers' client accounts are attractive to criminals as a conduit for transferring illicit money. Legal Professionals are generally perceived as trustworthy and respectable third parties and payments through such accounts therefore give the appearance of legitimacy, avoiding identification. Weaknesses in legal practices' policies, controls and procedures can expose legal practices to greater likelihood of their client accounts being exploited for ML/TF.

Sham Litigation

There is no evidence of sham litigation having occurred through the Gibraltar legal sector; however, Legal Professionals should be alive to the risk of their services being misused for sham litigation (i.e. fake lawsuits between collaborating parties to launder money as payment of damages). This risk concerns all Legal Professionals, not just those undertaking RFB.

Terrorist Financing Risk

The primary TF risks to Legal Professionals are of their inadvertent involvement in TF in relation to the:

1. misuse of client accounts;
2. purchase of real property;
3. creation of trusts;
4. creation, merger and acquisition of companies;
5. management of trusts and companies; and
6. setting up and managing charities.

However, there is no evidence to suggest that Gibraltarian legal practices' have been misused in relation to TF. Legal practices' policies, controls and procedures consistently refer to both TF as well as ML risks and onsite inspections by the LSRA seek to ensure effectiveness in both AML and CFT.

7.16 Auditors and Insolvency Practitioners

Auditors certify information by giving an independent expert opinion to improve an organisation's information or its context. In the case of a statutory auditor, they provide a legally mandated check of a company's financial statements and form an opinion on them. In some instances, they provide additional services, such as independent audits of policies, processes or procedures.

Insolvency practitioners are responsible for the orderly winding down of a company's activities. Most insolvency practitioners are court appointed and any liquidation or winding down of a company, is published in the Gibraltar Gazette.

The risk of auditors and insolvency practitioners in Gibraltar being used for ML/TF is low. Both auditors and insolvency practitioners are regulated by the GFSC and subject to the same regulatory scrutiny as other regulated entities. These firms also fall within scope of the POCA and are therefore, subject to all relevant AML/CFT requirements. Senior members of audit firms are required to be qualified accountants and members of international professional accounting bodies (such as ACCA and ICAEW). Gibraltar's audit offering comprises of companies which form part of global groups and a few smaller locally based firms. The ICAEW, on behalf of the GFSC, conducts reviews of the Gibraltar based audit firms and insolvency practitioners to ensure they are acting in line with the UK standards. The Auditors and Insolvency Practitioners in Gibraltar are represented by the Gibraltar Society of Accountants.

The supervisory authority for AML/CFT purposes for these sectors is the Gibraltar Financial Services Commission (GFSC). As at 31 December 2024 there were 16 audit firms and 48

individual statutory auditors, and 26 licensed insolvency practitioners. All individuals who are authorised to provide audit or insolvency services fall within the definition of a “relevant financial business” and are, therefore, caught by the POCA. Auditors and insolvency practitioners undergo regular onsite reviews by the GFSC’s AML/CFT Supervision team to assess and verify the regulated entity’s compliance with AML/CFT legislative requirements and thus mitigating potential risks. Where deficiencies in controls have been identified, the GFSC has worked with the entities in question in completing the tailored remediation plans. The GFSC has also issued targeted sector-specific guidance as part of its industry engagement. The risk posed by auditors and insolvency practitioners continues to remain as low.

Data obtained by the GFSC from its Annual Financial Crime Return for the 2024 reporting period and as set out in the table below, shows that 96% of the clients within the audit and insolvency practitioner sectors are incorporated in Gibraltar which further reduces the risk posed by these sectors in that the risk is contained within the jurisdiction. Additionally, 30% of all clients under Gibraltar Auditors are GFSC regulated entities which mitigates the risk further.

ML Threat and Vulnerability

Any company with a turnover of over £1.5million is required to file audited financial statements with Companies House. The relatively high exemption threshold in place acts as a deterrent on the basis that companies of this size are more likely to have robust internal accounting procedures, making it harder to hide large scale laundering and therefore, decreasing the ML risk. Criminals who attempt to stay under the threshold for audit purposes would still be caught by the regulated accountancy sector and therefore subjected to the same due diligence requirements as an audit firm.

A contributing factor of lower risk is that the majority of audit firms operating in Gibraltar primarily serve local clients. Additionally, all regulated financial services firms, regardless of their turnover, are obligated to be audited and submit audited financial statements to the GFSC for review. As financial services play a significant role in Gibraltar's economy and contribute substantially to its Gross Domestic Product (GDP), the risk is somewhat mitigated.

The overall risk is considered low due to the regulatory scrutiny imposed on audit firms and the large exemption threshold. Generally speaking, companies that seek to launder money would deem it unappealing to hit the exemption threshold and therefore be subjected to an audit.

Insolvency practitioners are associated with a relatively low risk of ML because once a company enters into liquidation, the focus is typically on fulfilling payments to creditors. Although these practitioners play a vital role in detecting potential ML activities, it is typically uncommon for this sector to be exploited for such purposes and we have not identified any factors in Gibraltar to suggest otherwise. Insolvency practitioners are subjected to the same regulatory scrutiny as other relevant financial businesses which mitigates this risk further.

TF Threat and Vulnerability

The risk of audit firms and insolvency practitioners being exploited for TF is deemed low because they are required to be authorised and supervised by the GFSC and because of the nature of scrutiny involved in an auditor’s and insolvency practitioner’s functions. Additionally, audit firms in Gibraltar primarily serve local clients mitigating any risk further.

The exemption threshold makes it less appealing for terrorist groups to engage in large scale operations or regulated financial services firms which are subjected to auditing requirements. To avoid audits, such groups would typically opt for smaller turnovers which

may present a risk for accountants but not necessarily for auditors. Gibraltar has no known terrorist organisations operating within its borders, contributing to the overall low risk associated with this sector. We continue to assess that audit and insolvency services are not attractive for TF and there remains no evidence of these services being abused for TF purposes.

Threat and Vulnerability Assessment

The overall threat and vulnerability for the sector is considered to be low on the basis of the exemption requirements and regulatory scrutiny.

7.17 Accountants

Accountants play a crucial role in managing and maintaining financial records and information for businesses, organisations, and individuals. Accountants are responsible for various financial tasks and hold a significant role in helping businesses make informed financial decisions. Accountants in Gibraltar are generally responsible for the following:

- Financial Recording and Reporting: Keeping records relating to financial transactions, including income, expenses, assets, and liabilities. They maintain accurate and up-to-date financial records;
- Bookkeeping: Handling bookkeeping tasks, which involve recording daily financial transactions and reconciliations;
- Financial Analysis: Analysing financial data to provide insight into a company's financial performance and health. Within this, they may also assist with data entry, manage risk and comment on the sustainability and going concern of a company or individual.

Accountants are required to register with the GFSC under the Proceeds of Crime Act 2015 (Relevant Financial Business) (Regulations) 2021 in order to provide these services to clients. As part of the registration and ongoing supervision processes, accountants must be able to demonstrate compliance with the Proceeds of Crime Act 2015 and are subjected to the same AML/CFT/CPF-related requirements as any other relevant financial business. The accounting sector in Gibraltar is represented by the Gibraltar Society of Accountants.

The GFSC currently has 29 registered accountants following the implementation of the registration regime in 2021. The majority of accountants based in Gibraltar generally onboard small local businesses and sole traders with a view to providing services such as bookkeeping and compilation reports. As provided in the GFSC's Financial Crime Return for the 2023 reporting period, 97.5% of all corporate customers who request services from accountants are incorporated locally. The jurisdiction also has several accountants and tax advisors which form part of larger regulated firms, such as Trust & Corporate Service Providers and Audit firms.

Composition and size of the DNFBP Sector - Accountants	
Total number of accountants, of which:	28
Provide services covered by the FATF Standards, of which:	
Accountants as sole practitioners	7
Accountancy firms / partnership, of which:	21
Belong to international groups or networks	3
Total number of clients	1,499

TABLE 34 - MATERIALITY OF ACCOUNTANT SECTOR AS AT DECEMBER 2024

ML Threat and Vulnerability

Perpetrators may use or require the services of accountants in order to effectively launder funds. Generally, when the sector is utilised for this purpose, there is some level of involvement by the professionals themselves with an aim to:

- misuse client accounts;
- purchase real estate;
- undertake certain litigation, set up and manage charities;
- arrange over or under-invoicing or false declarations for import/export goods;
- provide assurance; and/or
- provide assistance with tax compliance.

Professionals can be involved in the laundering process to various degrees. They can be consulted for advice on how to circumvent specific legal frameworks and how to avoid triggering red flags put in place by financial institutions. They can also take a more proactive approach by directly assisting or orchestrating the laundering process. Often, however, perpetrators seek to involve accountants because the services they offer are essential to a specific transaction and they add respectability to that transaction.

Experts in these areas are among the professionals which can be misused by organised crime groups to launder criminal proceeds due to the types of services that they can provide to their clients. They devise corporate structures, design accounting systems, provide bookkeeping services, prepare documentation (financial statements or references, income and expense sheets) and provide general accounting advice. Through these services, some accountants can help organised crime groups obscure their identity and the origin of the money that they handle.

Most of these services are used for legitimate purposes, however, they can also support a large range of money laundering schemes. These include fraudulent trading, false invoices, preparation of false declarations of earning, fraudulent bankruptcy, tax evasion and other types of abuse of financial records.

In Gibraltar, accountants face a significant risk related to placing reliance on pre-defined knowledge of an individual and not seeing the need to apply appropriate customer due diligence measures. To address this issue, the GFSC is actively collaborating with the accountancy sector to promote awareness about the requirements outlined in the Proceeds of Crime Act 2015.

The GFSC has recently started conducting onsite visits of accountants and many of these entities had findings in relation to the Proceeds of Crime Act 2015. The GFSC is currently working closely with these entities to enhance the standard of compliance within the sector. Due to the number of firms requiring remediation, the vulnerability score for these sectors has been increased.

Furthermore, the use of cash heightens the threat of money laundering. The anonymity of cash transactions makes it easier to obscure the origin of funds and funnel them through legitimate businesses to legitimise illicit money. The accountancy sector is one in which cash-based businesses may be able to hide and manipulate the origin of the funds given an accountant's involvement in the preparation of accounting records or returns for cash-intensive businesses. In response to this concern, the GFSC has issued comprehensive guidelines for all sectors with a view to mitigate risks associated with cash transactions and cash-intensive businesses.

TF Threat and Vulnerability

Accountants can inadvertently become vulnerable to terrorist financing due to the nature of their work involving financial transactions and their access to sensitive financial information.

Although the risk of terrorist financing taking place via a Gibraltar based accountancy firm or tax advisor is low, firms may be used to conceal or hide any transactional activities relating to terrorist organisation and groups. Any accountancy firm or tax advisor is required to have in place a risk-based approach in respect of the countries, nationality and residency involved in any of its business relationships and ensure that when reviewing the movement of funds these fall in line with the expected activity.

The vast majority of accountants within Gibraltar will only onboard locally based clients and presently there is no terrorist organisations or group identified to be operating from or within Gibraltar. Over 93% of clients onboarded within Gibraltar based accountancy firms are not resident within conflict zones. All clients which are resident in these zones are categorised as high risk and thus subjected to enhanced due diligence measures therefore mitigating this risk substantially.

ML Typologies

Whilst the jurisdiction has limited cases in respect of money laundering relating to the accountancy sector, the main threat posed is the knowledge of individuals personally and the willingness to provide services on the basis that the individual is well known and well respected within the community. This poses a threat on the basis that the accountancy firms in question may not conduct adequate customer due diligence or use the pre-defined knowledge in order to risk score the client. This may lead to insufficient periodic reviews of client accounting records take place or that the professionals involved do not report any suspicions to the relevant authorities.

Gibraltar is a jurisdiction which still uses cash and accepts GBP and Euros. The cash-based nature is very much down to tourism, construction and cross border workers. There is an inherently higher risk that firms which provide accountancy services to cash-intensive businesses (such as restaurants, retail shops or bars) may be used to facilitate the layering and integration stages of money laundering by making the cash proceeds appear legitimate.

Threat and Vulnerability Assessment

The vulnerability for this sector in Gibraltar has been increased due to the number of findings from supervisory onsite visits leading to the GFSC's enhanced supervisory programme of this sector. Whilst the majority of accountants primarily perform book-keeping functions, the risk has also been increased on the basis that these services are largely provided to cash intensive businesses. The jurisdiction has only a few tax advisors which generally form part of larger regulated firms.

7.18 Tax Advisors

Tax Advisors, as defined under the Proceeds of Crime Act 2015 (Relevant Financial Business) (Registration) Regulations 2021 (POCA Registration Regulations), extends to both an individual or corporate entity which undertakes to provide, directly or through a third party, material aid, assistance or advice in connection with the tax affairs of its clients. Tax Advisors specialise in providing guidance on tax-related matters to individuals, partnerships, trust, foundations, funds and companies. The main tax related activities provided in Gibraltar can be grouped as follows:

- Tax compliance: preparation of tax returns, social security and payroll, compliance with various statutory reporting, registration or publication requirements; and/or
- Tax advisory: advice on specific tax-related questions that do not occur on a regular basis (e.g. inheritance, mergers or spin-offs, insolvencies, setting up of a company, relocation and residency, purchase and/or disposal of immovable property), tax investigation, tax planning/tax optimisation.

Tax Advisors fall within the definition of a “relevant financial business” as set out in Section 9(1) of POCA. Since the implementation of the POCA Registration Regulations, all natural and legal persons undertaking tax advisory activity are required to register with the GFSC for AML/CFT/CPF supervision purposes.

There are currently 14 registered Tax Advisors following the implementation of the registration regime in 2021. The nature and scope of the POCA Registration Regulations only captures those that are providing solely tax advisory work as opposed to businesses in other sectors operating in Gibraltar which also provide tax advisory services as an ancillary activity such as lawyers, accountants, auditors and TCSPs. These sectors are already regulated by respective Gibraltar supervisory authorities and therefore, subject to the full suite of AML/CFT/CPF requirements under POCA.

Gibraltar tax advisors mainly serve the local and UK markets, with over 85% of beneficial owners being resident in these jurisdictions. Only 1.87% of clients are based in high risk jurisdictions thus mitigating any potential risks.

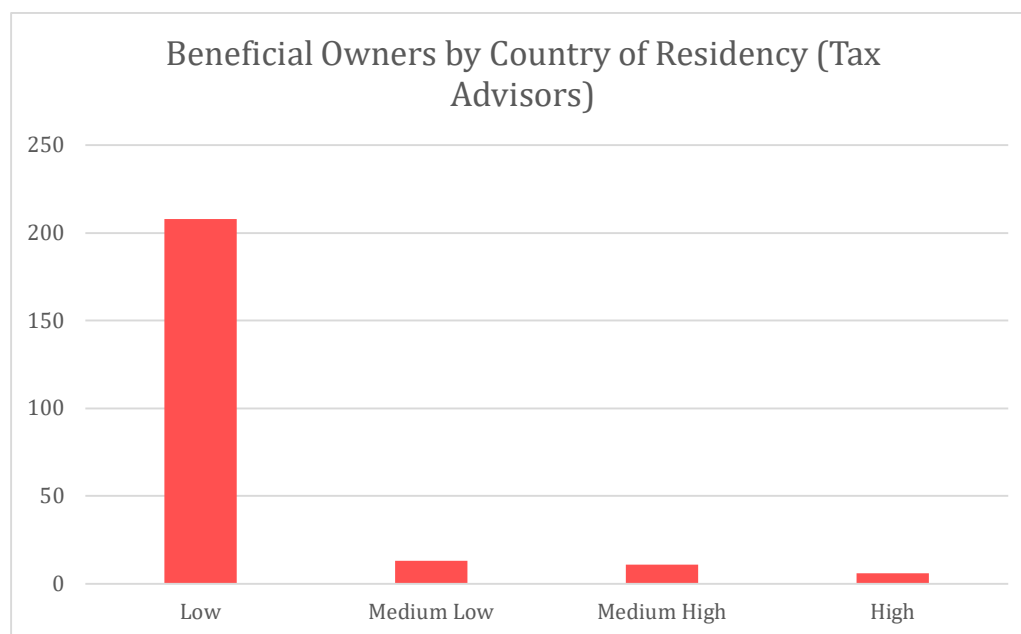


FIGURE 22 - TAX ADVISORS' CUSTOMER BENEFICIAL OWNERS AS AT 31 DECEMBER 2024

ML Threat and Vulnerability

Tax evasion and its proceeds is generally the area of most concern when related to Tax Advisors. Tax evasion is considered a predicate offence in Gibraltar and therefore, money saved and/or earned by tax evasion are considered the proceeds of crime. This coupled with the ability of Tax Advisors to design and implement cross border tax efficient structures creates a vulnerability for the jurisdiction stemming from the activities of Tax Advisors. Aside from direct tax evasion, perpetrators may use the services of Tax Advisors to assist in the laundering of funds by utilising the skills of a tax advisor to design and establish multiple cross border structures.

Where Tax Advisors are actively involved in money laundering, they may offer services to perpetrators related to:

- Misuse of client accounts (though it would be less likely that a Tax Advisor who is not part of a regulated entity of accountants or lawyers would have a client account);

- recommend the creation of trusts and companies;
- set up and/or manage charities;
- provide assurance; and/or
- provide assistance with tax compliance for structures involved in money laundering.

Despite the creation of trusts and companies and the use of client accounts being regulated activities and therefore falling within scope of relevant legislative provisions and the regulation by local supervisory authorities, this does not eliminate the risk of money laundering. Unless Tax Advisors take an expansive view of the effects of their actions there is a structural weakness in the system created by a lack of knowledge and expertise which will permit such services to be utilised for the purposes of tax evasion.

The nature of tax advice and its ancillary services is that without a holistic approach, Tax Advisors may fall into the trap of unknowingly participating in money laundering by giving limited advice and potentially adding credibility to the legitimacy of a structure. It is rare for other sectors (such as TCSPs) to have expertise and resources to review tax advice for quality and credibility and they therefore rely on the Tax Advisor's advice to tackle matters such as tax evasion. It should be noted that in the case of TCSPs, the GFSC's Annual Financial Crime Return data confirms that during the onboarding stage, the tax rationale is generally required to be documented before domiciling a company in Gibraltar.

Tax Advisors often form parts of regulated firms and therefore the relatively small number of firms which are pure tax Advisors mean that actual threat is limited by the small size of the sector. The sector is predominantly made up of Gibraltar and UK based clients.

Tax Advisors are still considered a relatively new sector in respect of applying adequate AML/CFT/CPF controls. The GFSC is working with the sector to ensure that prior to approval, applicants are aware of their legislative and regulatory obligations. Additionally, once authorised, the GFSC carries out a post authorisation onsite within six months to ensure the implementation of the controls are being applied in practice.

TF Threat and Vulnerability

Tax Advisors can inadvertently become vulnerable to terrorist financing due to the nature of their work involving financial transactions and their access to sensitive financial information. Although the risk of terrorist financing taking place via a Gibraltar based tax adviser is low, firms may be used to conceal or hide any transactional activities relating to terrorist organisation and groups. Tax advisors are required to have in place a risk-based approach in respect of the countries, nationality and residency involved in any of its business relationships and ensure that when reviewing the movement of funds these fall in line with the expected activity. The tax advisory service within Gibraltar does not currently service any clients who are resident in conflict zones.

7.19 Pensions Advisors and Pension Scheme Operators

A pension is a retirement plan that provides a fixed income to an individual after they retire from employment. It's usually funded through contributions made during a person's working years, either by the individual, the employer, or both. Pension plans are typically structured to pay out regularly (monthly or yearly) based on factors like years of service, salary history, and age at retirement. There are currently 8 Pension Advisors and 18 Pension Scheme Operators operating within Gibraltar. The pensions sector is authorised and regulated by the GFSC and fall within the definition of a relevant financial business under POCA, therefore, these regulated entities are subject to the full suite of AML/CFT requirements.

Pensions firms are generally not considered to pose a considerable threat for ML and TF on the basis that they serve as long term investment vehicles which can only be drawn upon shortly before retirement. These types of products are generally contributed to by the employer with the pension holder being able to add additional funds should they wish. Pensions are unique in so far as there are regulations which stipulate the use of these products and this can only be done once an individual reaches retirement age so the funds are not easily accessible. As pensions are administered by regulated entities, the entity takes care of any tax consequences.

Typically, the pensions sector in Gibraltar provides a range of pension products for both the local and global market. Firms usually act as trustee and administrators for these products. With some firms also providing advisory and investment services. Products aimed at the Gibraltarian market are mostly qualifying recognised overseas pension schemes (QROPS) and qualifying non-UK pension schemes (QNUPS), both of which are subject to strict UK tax regulations as well as local tax law and regulatory requirements covered under the Financial Services Act 2019.

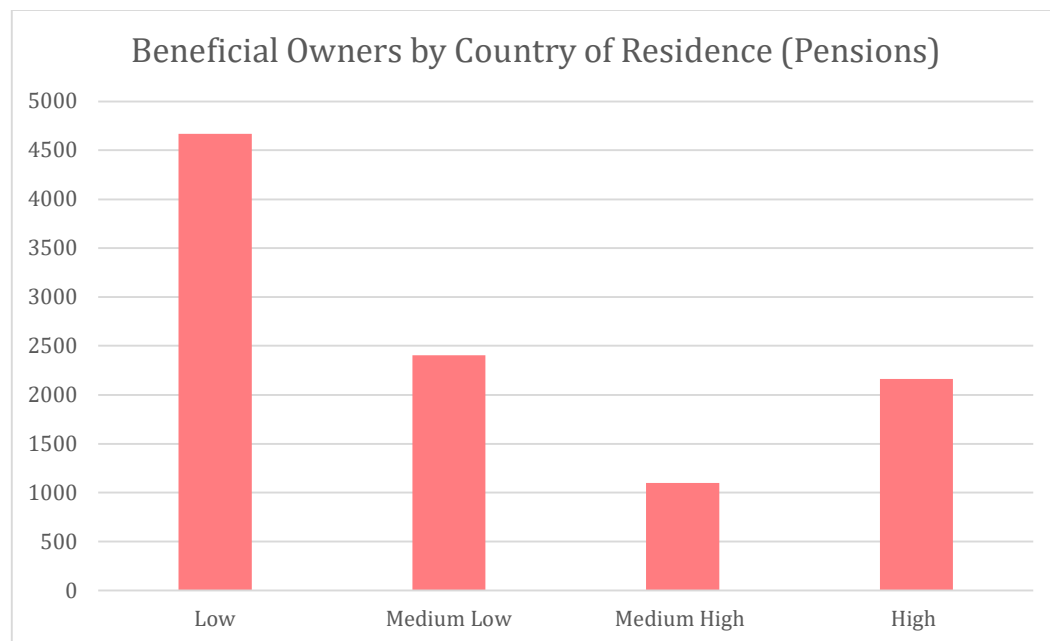


FIGURE 23 - BOS OF PENSION CUSTOMERS AS AT DECEMBER 2024

To obtain tax approval, Gibraltar pension schemes must be written under irrevocable trust as required by the Commissioner of Income Tax Guidance Notes. Most are written under discretionary trust, which is particularly relevant for QROPS and QNUPS, in a similar manner to UK registered pension schemes to benefit from UK IHT exemptions. In the case of QROPS and QNUPS, before the pension plan is transferred to Gibraltar, it will have previously been administered by a regulated pension scheme in the UK. Additionally, these types of pension products are subjected to scrutiny by UK's HM Revenue and Customs (HMRC), on an ongoing basis due to tax relief afforded from the UK government. Due to the continuous oversight of different regulators both within Gibraltar and in the UK, it is highly unlikely these products would be used to facilitate financial crime. Providers of occupational pension schemes are required to be authorised as professional trustees and are subject to Part 26 of the Financial Services Act 2019 and the Financial Services (Occupational Pensions Institutions) Regulations 2020. Conversely providers of QROPS, QNUPS and personal pensions are

authorised as pension scheme controllers and are subject to Part 27 of the Financial Services Act 2019 and the Financial Services (Personal Pensions) Regulations 2020.

This GFSC is due to conclude an AML/CFT/CPF Thematic Review in 2025 of the pensions sector, that will give the GFSC a better understanding of the systems of controls currently in place for Pension providers within Gibraltar.

ML Threat and Vulnerability

QROPS are funded from transfers of UK tax relieved pension savings from UK registered pension schemes and/or other HMRC recognised QROPS. Customer due diligence is undertaken on the ceding scheme, the member (the UBO) and financial adviser at onboarding and at relevant points during the business relationship, therefore, the risk of money laundering is extremely low. In addition, all QROPS are originally derived from pension contributions made in the UK and have previously been administered by a UK pension administrator. Since the introduction of more stringent regulations on QROPS, the schemes are also now only able to be held in the jurisdiction in which the client resides further mitigating the risk of ML.

QROPS members are able to make ad hoc contributions, and although this may pose a potentially higher risk, additional contributions are subjected to tax rules by HMRC. Additionally, some local pension scheme operators will not allow additional contributions.

TF Threat and Vulnerability

The likelihood of the pensions sector being utilised within Gibraltar for the purposes of terrorist financing is considered low. This is on the basis that the typologies related to TF are generally the movement of small amounts and the requirement of these funds to be accessed relatively quickly. The inherent nature of pensions business models, the long-term investment aspect and the regulation of pension products, makes this product unattractive to perpetrators for TF purposes. Within local regulated pensions entities, only 2.73% of pension customers reside in conflict zones mitigating this risk further.

7.20 Domestic Football League

The sporting industry is one of many sectors that could be attractive for criminals for money laundering purposes and merits closer consideration given its social and cultural impact, the large scale of monetary transactions, and the increase in the number of individuals involved.

Like many other businesses, sport and gambling have been used by criminals to launder money and derive illegal income. As in the art world, criminals in the sports world are not always motivated by economic gain. Social prestige, appearing with celebrities, and the prospect of dealing with authority figures may also attract private investors with dubious intentions.

Also, the use of non-financial professionals, such as family members, lawyers, consultants, and accountants as a means of creating structures to move illicit funds has also been observed by the Financial Action Task Force (FATF). The money stipulated in such image contracts (for exploitation of a player's personal appearance as part of an extensive advertising campaign) is often transferred to accounts of companies in third countries with serious risks of fraud. Advertising and sponsorship contracts can also be used for money laundering. Organized crime could sponsor sport and constitute a bridge to legitimate business. The most common form of payments involves jurisdictions located abroad, always as a way to hide the last destination.

The most common form of cash payments involves jurisdictions located abroad that allow the final destination of payments to be disguised. Image rights are also used to conceal the amounts actually paid to players.

In addition, gambling is directly linked to football through betting on games and matches.

The first document from the EU that recognised the importance of the sport was published in July 2007 (EU White Paper on Sport). It states that, *'sport is confronted with new threats and challenges, as commercial pressures, exploitation of young players, doping, corruption, racism, illegal gambling, violence, money laundering, and other activities detrimental to the sport'*.

Many factors have led to the use of illegal resources in football, not least its complex organisation and insufficient transparency.

The assessment of the TF threat arising from collecting and transferring funds in the football sector shows that this method of funding terrorism is not frequently used by terrorist groups. Indeed, no known cases of TF from money moved through the football sector exist.

Regulated entities which seek to onboard or already have business relationships with local football clubs as their clients should carefully consider the ML risks that these may pose when assessing the risk of the customer.

8 Jurisdictional Terrorist Financing Risk

There are no confirmed TF incidents in Gibraltar. However, the absence of known cases does not necessarily mean that there is a low risk. It is therefore important for operators to remain vigilant and continually monitor their TF exposure.

Gibraltar's geographic and demographic characteristics are such that it is less likely to be a jurisdiction in which terrorists raise funds or spend them for the purposes of carrying out an attack. Whilst such a possibility cannot be excluded, Gibraltar's main TF risk arises from its high levels of cross border business involving the movement of funds, which can manifest itself in one or more of the following ways:

- a. Flow-through, whereby Gibraltar is used as a transit country for funds intended for use in foreign terrorism;
- b. Service provision, whereby terrorist funds do not enter Gibraltar but where businesses in Gibraltar provide administration or other services to parties that support foreign terrorism, including internationally active domestic or foreign entities, politically exposed persons (PEPS) or high net worth individuals;
- c. The use of complex structures involving legal persons and legal arrangements to disguise the underlying beneficial owner who may be involved in terrorism or TF or feature on a terrorism related sanction list; or
- d. Abuse of Non-Profit Organisations (NPOs), whereby donations or aid that are sent to or administered from Gibraltar go to conflict zone or other high risk jurisdictions and are diverted to support foreign terrorism; At present there is little evidence to suggest that Gibraltar is being used to channel terrorist funds, however this does not obviate the need to remain aware of the threat and vulnerabilities faced by the jurisdiction.

For most sectors, the applicable regulatory regime will have gone a long way to addressing the vulnerabilities to a given threat, thereby reducing the overall risk posed. Nevertheless, no regulatory regime is capable of extinguishing all TF risk. This is especially so given that the sums involved in TF are usually much lower than for ML and terrorists and their financiers or sympathisers may be legal citizens who are as of yet unknown to any terrorist lists. They

are therefore often able to proffer seemingly legitimate explanations for their activity and pass CDD checks, thereby making TF activity extremely difficult to detect. Operators must therefore fully understand the nature of the TF threat they face through analysis of its known typologies and case studies to minimise the chances of any cases going undetected.

A crucial factor when considering the TF threat faced is the extent of any connection between Gibraltar and conflict zones or other high-risk jurisdictions. It is also important to appreciate the extent to which terrorism or TF is occurring in jurisdictions with which Gibraltar has close geographic and/or political links. Individual operators will need to consider the same at the organisational level when conducting their own risk assessments.

8.1 Extreme Right-Wing Terrorism

Whilst the main focus in analysing the threat of small cells and lone actors has traditionally been on Jihadist terrorism, which accounts for the largest number of attacks, the threat posed is by no means confined to a particular religion or ideology, and it is important to note in particular the proliferation of extreme right-wing terrorism in recent years.

Extreme right-wing terrorism (also referred to as ‘far right, or ethnically and racially motivated terrorism’) is not a new phenomenon but there has been a recent revival of right-wing extremist groups and an increase in frequency of attacks, with deadly results. Whilst the overall threat of TF in Gibraltar at a jurisdictional level remains low, the risk is higher for specific sectors of the economy or when dealing with certain jurisdictions.

A large number of extreme right-wing attacks in Europe have been committed by groups or individuals that may not necessarily be connected to known extreme right-wing groups or networks. As a result, the threat from small cells or lone actors becomes more prevalent.

8.2 Likelihood of a terrorist attack in Gibraltar

The Threat Level from an international terrorist attack in Gibraltar is currently assessed as Moderate, ‘an attack is possible but not likely’. This is set by the Gibraltar Contingency Council regularly reviewed based on the latest information and intelligence.

Whilst there has not been an actual terrorist attack in Gibraltar, such an attack can’t be ruled out considering the heightened threat globally against UK interests and British nationals from groups or individuals motivated by the conflict in the Middle East. There therefore remains the possibility that a small cell, lone actor or TO may move funds into Gibraltar with a view to using them to fund a local attack. Threat levels are designed to give a broad indication of the likelihood of a terrorist attack.

8.3 Hawala

Hawala is a system of money transmission which arranges the transfer and receipt of funds or equivalent value. It is often reliant on ties within specific geographical regions or ethnic communities. These movements of value may be settled through trade or cash businesses engaged in remittance activities and often operate in areas of expatriate communities. Informal systems of value transfer, like Hawala, can be used for legitimate purposes, like money remittances, but also for criminal ones. Whilst the Hawala method may be considered high risk for ML/TF purposes, Gibraltar does not have members of diaspora and migrant communities where this system would be more commonly found and local law enforcement has not found evidence to suggest that Hawala systems operate from Gibraltar, therefore, the risk posed is decreased. GFIU data shows that Hawala transmissions have not been reported locally.

8.4 Abuse of Non-Profit Organisations

NPOs are a vibrant and integral part of the contemporary global environment and play a significant role in combatting terrorism. However, organisations and individuals have in the past taken advantage of the NPO sector to support those who engage in terrorism or support to terrorist organisations.

Gibraltar's NPO sector is large and varied with nearly 300 registered charities and a dozen Friendly Societies. Many are small charities used for single purposes or causes. Others have a wider scope and serve both the local community as well as specific projects outside of Gibraltar. Some of these charities, however, are relatively large and may present a higher TF risk. In the analysis of the NPO sector undertaken in 2017, data as to inflows and outflows of donations and charitable work showed that most charitable donations were from Gibraltar itself followed by the UK, Switzerland, and Israel. The charities' work, however, were based mainly in Israel, UK, and Gibraltar. When analysed further the results of the donation base and the activity of the charity are commensurate with the activities of the locally based charities which are either offshoot or UK based charities or where substantial educational grants are provided. It must be noted that after the significant earthquake on 8th September 2023 an increase in charitable donations were made to the Moroccan community.

The overall risk in Gibraltar of abuse of NPOs for terrorist purposes has been assessed as low. This assessment is based on a previously conducted Sectorial Assessment and whilst this may have been some time ago, the demographics and nature of the activity of the sector has not suffered any major changes. The Charities Commissioners have confirmed this to be the case. A separate update sectorial assessment is due to be conducted in early 2025.

Taking the FATF definition of what constitutes an NPO that is at risk of TF there will be NPOs in Gibraltar who meet the criteria who "primarily engage in raising or disbursing funds." The most obvious category for this will be organisations that are registered charities under the Charities Act. The FATF Definition does not cover all these Charities as they may not conduct significant international activities or be of a substantial nature.

A second category that should be considered, at least initially, to fall into scope of the Risk Assessment are Friendly Societies that are registered under the Friendly Societies Act. Again, it is important that their international work and size are determined to determine whether they fall within the scope of the FATF definition.

As part of this Risk Assessment, Sporting Clubs and Societies as well Cultural Organisations were examined using open source information and all of those named organisations discarded as not meeting the FATF scoping definition.

Gibraltar's NPO sector is large and varied with nearly 300 registered charities and a dozen Friendly Societies. The key change, as a result of the revised FATF standards, is to identify the subset of NPOs which represent a higher risk of TF abuse.

As can be imagined these serve a large variety of uses, many being small charities used for single purposes or causes. Others have a wider scope and serve both the local community as well as specific projects outside of Gibraltar. Some of these charities, however, are large in comparison to the general pattern observed, some of which may present a higher TF risk to the jurisdiction.

There is no intelligence data arising from MLA requests or SAR disclosures which points to any of those organisations being used for ML or TF activities.

9 Sanction Circumvention Risk

Sanctions play a vital role in the enforcement of international law, maintaining global security and upholding human rights. Under Gibraltar's legal framework, the Sanctions Act 2019 establishes the basis for implementing sanctions regimes derived from the United Nations (UN), the European Union (EU), and the United Kingdom (UK). As a British Overseas Territory and an international financial centre, Gibraltar is obligated to comply with these sanctions to ensure the integrity of its jurisdiction and its global reputation.

9.1 Gibraltar's Obligations to Comply with Sanctions Regimes

The Sanctions Act 2019 (SA 2019) was enacted to provide a comprehensive legal basis for the administration and enforcement of sanctions within Gibraltar. Sanctions, whether financial, trade-related, or otherwise, are integral tools employed to achieve foreign policy objectives, combat terrorism, and prevent human rights abuses. The SA 2019 imposes obligations on all entities operating within Gibraltar, particularly regulated entities, including financial institutions and designated non-financial businesses and professions (DNFBPs).

Compliance with the United Kingdom's Sanctions

The UK's sanctions are directly applicable to Gibraltar under the SA 2019. Gibraltar aligns with the UK's sanctions framework, which is administered under the UK's Sanctions and Anti-Money Laundering Act 2018 (SAML 2018). UK sanctions are often aligned with EU and UN sanctions but may be more restrictive in some cases to reflect national security priorities.

Compliance with the European Union's Sanctions

Despite leaving the EU, Gibraltar must remain cognizant of EU sanctions, particularly due to its significant economic and financial ties with EU member states. Regulated entities must ensure compliance with overlapping regimes to avoid inadvertent breaches, particularly where cross-border financial transactions are concerned.

Compliance with United Nations Sanctions

UN sanctions, imposed by the Security Council under Chapter VII of the UN Charter, are binding on all member states, including the UK and, by extension, Gibraltar. These sanctions form the foundation of global efforts to restrict the actions of entities or individuals threatening international peace and security. Regulated entities in Gibraltar are required to screen their transactions and clients to ensure adherence to these measures.

9.2 The Role of Regulated Entities in Preventing Sanctions Circumvention

Regulated entities play a frontline role in implementing sanctions and ensuring that Gibraltar's compliance framework remains robust. These entities are required to undertake due diligence, maintain robust screening mechanisms, and report suspicious transactions to the Gibraltar Financial Intelligence Unit (GFIU). For example, regulated entities must freeze assets belonging to designated persons or entities, must ensure that they do not facilitate the management of assets for sanctioned individuals.

The Importance of Preventing Sanctions Circumvention

The prevention and detection of sanction circumvention are essential to maintaining the integrity of the sanctions system and ensuring that Gibraltar upholds its international

commitments. Failure to prevent circumvention can lead to severe consequences, including reputational damage, economic penalties, and the erosion of the jurisdiction's credibility.

International Reputational Risk

As an international financial centre, Gibraltar's reputation relies on the integrity of its regulatory framework. Non-compliance or lapses in enforcement could result in Gibraltar being perceived as a haven for illicit financial activities, potentially leading to blacklisting by global regulatory bodies.

Financial and Legal Penalties

Entities that fail to comply with sanctions face significant financial penalties and potential legal action. Moreover, systemic failures could attract international scrutiny and sanctions against Gibraltar itself.

Upholding International Security and Human Rights

Sanctions are a key instrument for curtailing the actions of rogue states, terrorist organizations, and individuals involved in serious human rights abuses. Circumvention undermines these objectives and weakens the collective efforts of the international community.

Conclusion

Gibraltar's strategic position as a British Overseas Territory with significant economic ties to the EU necessitates robust compliance with UK, EU, and UN sanctions. Regulated entities, as critical nodes in the financial and corporate sectors, bear the primary responsibility for implementing and enforcing these measures. The importance of preventing sanctions circumvention cannot be overstated, as lapses threaten Gibraltar's reputation, economic stability, and the effectiveness of international sanctions regimes. Thus, a vigilant, well-regulated approach is essential for ensuring that Gibraltar continues to meet its international obligations while fostering trust and transparency in its financial and corporate sectors. The SA 2019 includes offences for being in breach of the terms of a licence issued under that Act, as well as a general offence where any person (regulated or otherwise, and to the extent they are not operating under the terms of a licence granted under the Act) undertakes conduct that the person knows or ought reasonably to know- (a) breaches or will cause a breach of any international sanctions; (b) assists in the breach of international sanctions⁸.

Summary of Country Based Sanctions

The following table summarizes countries subject to sanctions by the United Nations (UN), the United Kingdom (UK), and the European Union (EU), along with a brief description of the scope and breadth of their sanctions regimes:

⁸ in Part 2 of SA 2019 "international sanctions" means (a) any restrictive measures imposed by the United Nations Security Council "UN sanctions"; (b) any restrictive measures imposed by the European Union "EU sanctions"; (c) any restrictive measures imposed by means of a designation, within the meaning of the Terrorist Asset-Freezing etc. Act 2010 (c.38) of the United Kingdom; (d) any restrictive measures imposed by an organisation that is notified by the Government by notice published in the Gazette, (e) any restrictive measures imposed by the United Kingdom under the Sanctions and Anti-Money Laundering Act 2018 (c.13), in their up-to-date versions as in force at the time of reference.



Country	Sanctions by	Scope and Nature of Sanctions
Russia	UN (limited), UK, EU	Comprehensive sanctions include asset freezes, trade restrictions (energy, defence, tech), financial sector limits, and travel bans, primarily in response to the Ukraine conflict and human rights abuses GOV.UK Sanctions Map
Iran	UN, UK, EU	Focused on nuclear proliferation, including arms embargoes, asset freezes, and bans on technologies supporting nuclear development or repression GOV.UK European Data Portal
North Korea (DPRK)	UN, UK, EU	Broad sanctions targeting nuclear weapons development, trade restrictions, arms embargoes, and financial measures United Nations Sanctions Map
Syria	UN, UK, EU	Measures include asset freezes, trade embargoes on military goods, and restrictions related to repression and human rights violations Sanctions Map United Nations
Belarus	UK, EU	Sanctions include asset freezes, financial restrictions, and measures targeting repression and involvement in the Ukraine conflict GOV.UK Sanctions Map
Myanmar (Burma)	UK, EU	Targeted sanctions address repression, human rights violations, and arms embargoes against the military junta GOV.UK Sanctions Map
Yemen	UN, UK, EU	Focused on arms embargoes and asset freezes targeting individuals and entities fuelling the conflict United Nations Sanctions Map
Libya	UN, UK, EU	Targeted measures against entities involved in conflict, including arms embargoes and financial restrictions United Nations Sanctions Map
Central African Republic (CAR)	UN, UK, EU	Sanctions include arms embargoes and targeted asset freezes related to ongoing conflict and humanitarian issues

Country	Sanctions by	Scope and Nature of Sanctions
South Sudan	UN, UK, EU	United Nations Sanctions Map Restrictions focus on arms embargoes and individuals undermining peace and security
Democratic Republic of the Congo (DRC)	UN, UK, EU	United Nations Sanctions Map Arms embargoes and targeted sanctions on individuals contributing to conflict
Somalia	UN, UK, EU	United Nations Sanctions Map Measures target arms embargoes and entities linked to terrorism and destabilization

TABLE 35 - SUMMARY OF COUNTRIES SUBJECT TO SANCTIONS REGIMES (UK, EU AND UN)

This list reflects the most prominent regimes as of November 2024. UN sanctions are typically more limited, focusing on international peace and security, while UK and EU sanctions often have broader scopes, addressing regional stability, human rights, and global security.

Scope of Sanctions

United Kingdom

The UK's sanctions regime is governed by SAMLA 2018, which came into effect after Brexit.

The United Kingdom's sanctions regimes represent a cornerstone of its foreign policy and efforts to maintain international peace and security. Administered by the Office of Financial Sanctions Implementation (OFSI), these measures address threats such as regional instability, human rights abuses, and the proliferation of weapons of mass destruction. While sanctions targeting specific individuals, entities, and proscribed organisations often capture public attention, the broader prohibitions affecting entire countries are equally significant. These sanctions, implemented under the authority of SAMLA 2018 and related statutory instruments, aim to alter the behaviour of states that violate international norms or threaten global stability.

A major category of sanctions imposed by the UK on countries involves trade restrictions. These sanctions often prohibit the export and import of goods, services, and technologies to and from the sanctioned state. For example, the export of military and dual-use goods, which have both civilian and military applications, is tightly controlled. Dual-use technologies, such as encryption software or certain chemical substances, are commonly restricted because of their potential use in weapons development or surveillance systems. Export controls may also encompass items critical to the development of advanced infrastructure in targeted countries, including telecommunications and energy equipment. These measures are designed to deprive the sanctioned country of resources that could be used to sustain hostile actions or undermine international peace.

Import restrictions similarly target the economic lifelines of the sanctioned state. Goods originating from the targeted country are often banned to limit its access to global markets. A notable example is the prohibition of energy imports from Russia in response to its invasion of Ukraine, including crude oil, natural gas, and coal. In many cases, import bans are expanded to luxury goods and other commodities that generate significant revenue for the sanctioned government. The intention is to weaken the economic foundation of regimes that engage in unacceptable conduct while minimising harm to the civilian population.

The sanctions regime also extends to the prohibition of services that facilitate trade and economic activity. These restrictions typically encompass financial, insurance, and logistical services related to the movement of restricted goods. For instance, UK-based insurers are forbidden from underwriting cargo shipments involving goods subject to sanctions, while financial institutions are barred from providing credit or guarantees to support such transactions. By cutting off access to vital services, these measures amplify the impact of trade restrictions.

Financial sanctions are another critical element of the UK's country-focused sanctions regimes. These measures are broader than the targeted freezing of assets belonging to specific individuals or entities. They often include restrictions on financial transactions that could benefit the sanctioned state. A common feature is the prohibition of dealings in government bonds or other sovereign debt instruments issued by the targeted country. Such restrictions impede the state's ability to raise funds in international capital markets, limiting its financial flexibility. In some cases, the UK imposes comprehensive asset freezes on the central government of the sanctioned state, preventing access to funds held in UK jurisdictions.

Prohibitions on sovereign lending and financial assistance are also central to the UK's financial sanctions regime. These measures restrict the provision of loans, credits, or other forms of economic support to the governments of sanctioned countries. This form of financial isolation seeks to pressure governments into altering their policies or behaviour by denying them access to much-needed external funding. These restrictions often extend to public financial institutions, which are barred from facilitating trade or development projects involving the sanctioned state.

Sanctions affecting countries are not limited to the economic sphere. They often include transportation and communication bans that further isolate the targeted state. Airspace restrictions are a frequent feature, prohibiting airlines from the sanctioned country from operating in UK airspace or landing at UK airports. Similarly, shipping restrictions may apply, preventing vessels flagged, owned, or operated by the targeted state from docking at UK ports. These measures, while symbolic in some respects, also serve to disrupt the logistical networks that sustain the sanctioned regime's economy.

In addition, sanctions regimes frequently include prohibitions on technical assistance, advisory services, and training. These measures are particularly relevant in the context of dual-use technology and military applications. UK-based firms and individuals are prohibited from providing expertise that could enhance the sanctioned state's military or industrial capabilities. By denying access to such knowledge, the sanctions aim to limit the technological advancement of the targeted country in areas that pose a threat to international peace and security.

The UK's sanctions regimes are designed to balance effectiveness with legal and procedural safeguards. These measures are developed in coordination with international partners, including the European Union and the United Nations, to ensure alignment and avoid duplication. Despite their focus on governments, UK sanctions often include exemptions for humanitarian assistance to minimise harm to ordinary citizens. For example, licences may be

issued to facilitate the delivery of medical supplies or food aid to the sanctioned country, provided such activities do not undermine the sanctions' objectives.

In conclusion, the UK's sanctions regimes against countries involve a complex array of prohibitions aimed at constraining the economic and political actions of targeted states. These measures encompass trade restrictions, financial sanctions, and bans on technical assistance, transportation, and communication. While these sanctions are primarily tools of foreign policy, their implementation requires a careful balance between achieving strategic objectives and ensuring compliance with legal and humanitarian standards. By leveraging these sanctions, the UK seeks to uphold international norms and contribute to global security, often in concert with its allies and international organisations.

European Union

EU sanctions are part of its Common Foreign and Security Policy (CFSP) and are binding on all member states. Decisions on sanctions require unanimity among EU members, leading to a more consensus-driven but slower decision-making process. EU sanctions typically focus on broader international issues, such as conflict resolution, counter-terrorism, or responses to human rights violations. As a supranational entity, the EU enforces sanctions through regulations that are directly applicable to member states, ensuring uniformity across the bloc.

EU sanctions tend to prioritise trade restrictions, asset freezes, and visa bans. However, the EU often adopts less aggressive financial sanctions compared to the UK and US, partly due to the need for consensus and the varied economic interests of its member states. For instance, while the EU imposed significant energy-related sanctions on Russia, certain measures, such as gas imports, were subject to prolonged negotiations and compromises to accommodate member states reliant on Russian energy.

United Nations

The UN's sanctions are fundamentally international in scope, focusing on issues such as nuclear non-proliferation, counter-terrorism, and the prevention of mass atrocities. Sanctions are imposed through UN Security Council (UNSC) Resolutions, which require the agreement of all five permanent members (China, France, Russia, the UK, and the US). This requirement often limits the scope of UN sanctions due to political vetoes.

UN sanctions tend to be more targeted and narrowly focused, emphasising measures such as arms embargoes, travel bans, and asset freezes on specific entities or governments. Broader economic sanctions, such as trade embargoes, are less common, reflecting the UN's aim to avoid humanitarian consequences. For instance, sanctions against North Korea focus heavily on restricting its nuclear weapons programme while allowing humanitarian exemptions for food and medical aid.

UK versus EU and UN Country Sanctions

The UK, European Union (EU), and United Nations (UN) each implement sanctions regimes to address global threats, but their scope and approach differ significantly due to variations in institutional frameworks, geopolitical priorities, and decision-making processes. While they often collaborate on sanctions, particularly in cases involving international crises, the differences between their systems reveal important distinctions in how these entities enforce and administer sanctions against countries. These differences reflect their varying legal mandates, political dynamics, and strategic interests.

Approach to Implementation and Flexibility

United Kingdom

Post-Brexit, the UK's approach to sanctions has become more dynamic and independent. SAMLA 2018 allows the UK to impose sanctions autonomously, with an emphasis on targeted measures that align with its national interests. The UK has shown a willingness to act unilaterally or in concert with like-minded partners, such as the US and Canada, even if these actions diverge from EU or UN measures. This autonomy has enabled the UK to act swiftly, such as its robust sanctions against Russia following the 2022 invasion of Ukraine, which included early bans on the import of Russian oil and restrictions on sovereign debt.

The UK's Magnitsky sanctions are a notable innovation, focusing on human rights violations and corruption. These sanctions are often broader in scope than the EU's equivalent measures, reflecting the UK's efforts to position itself as a global leader in the fight against abuses.

European Union

The EU's sanctions framework prioritises cohesion among its member states, resulting in a more structured but sometimes slower approach. The requirement for unanimity in the CFSP means that EU sanctions are often the product of compromise, balancing the diverse economic and political interests of its members. This consensus-driven approach can limit the scope and speed of sanctions but ensures uniform enforcement across all 27 member states.

The EU frequently uses sectoral sanctions, targeting specific industries in a sanctioned country. For example, its sanctions on Russia after 2014 and 2022 focused on energy, defence, and finance, balancing the need to punish Russian aggression with the economic realities of member states dependent on Russian resources. While the EU's measures are often aligned with the UK and US, they sometimes reflect more cautious or delayed implementation, as seen in its gradual adoption of oil and gas embargoes.

United Nations

The UN's sanctions approach is fundamentally multilateral, focusing on building global consensus. Sanctions are designed to enforce international norms, such as nuclear non-proliferation treaties or arms control agreements. However, the requirement for unanimity among UNSC permanent members often limits the scope and applicability of sanctions, as geopolitical rivalries can lead to vetoes. For instance, efforts to impose comprehensive sanctions on Syria have been blocked repeatedly by Russia and China.

UN sanctions are typically targeted to minimise humanitarian consequences. This approach reflects the UN's global mandate and its focus on avoiding disproportionate impacts on civilian populations. The UN also emphasises mechanisms for humanitarian exemptions, ensuring that sanctions do not impede access to essential goods and services.

Key Differences in Geopolitical Priorities

The UK, EU, and UN differ in their geopolitical priorities and strategic focus. The UK often uses sanctions as an extension of its foreign policy, targeting regimes that threaten British interests or values. For instance, its robust sanctions on Belarus and Myanmar reflect a focus on human rights and democratic governance. The EU, on the other hand, tends to prioritise regional stability and the interests of its member states, leading to a more measured approach. UN sanctions, as a global framework, are broader in their application but limited by the need to achieve consensus among diverse stakeholders, including states with conflicting interests.

9.3 Compliance and Enforcement Mechanisms

The UK enforces sanctions through the OFSI, which has significant powers to monitor, investigate, and penalise violations. Its ability to impose large fines and ensure compliance has made the UK a leader in sanctions enforcement. The EU relies on member states to enforce sanctions domestically, which can lead to variations in implementation and effectiveness. In contrast, the UN depends on member states to adopt its sanctions into national law, resulting in uneven enforcement due to differing political will and capacity.

9.4 Conclusion

The UK, EU, and UN sanctions regimes share a common goal of promoting international peace and security but differ in their scope, approach, and enforcement. All three regimes apply in Gibraltar under the provisions of SA 2019. The UK's post-Brexit autonomy allows it to act decisively, often aligning with like-minded partners while maintaining flexibility. The EU's consensus-driven framework ensures cohesion but can lead to slower, more cautious measures. Meanwhile, the UN's global mandate prioritises multilateralism and targeted sanctions but faces limitations due to political dynamics in the Security Council. Together, these regimes reflect the complexity of modern sanctions as tools of diplomacy and enforcement.

As a result of the risk that transactions with any country to whom the UK, EU or UN sanctions apply, the 2025 NRA requires regulated firms to treat all of the countries in the table above, as High Risk.

10 Proliferation Financing

Background

The financing of the proliferation (PF) of weapons of mass destruction (WMD) which include chemical, biological, radiological and nuclear (CBRN) weapons has increasingly attracted international attention in recent years, largely due to the high-profile actions of proliferation actors such as the Democratic People's Republic of Korea (DPRK) and Iran. Proliferators rely upon the global financial system to procure the items and technology required for the manufacture, acquisition, possession, development, export, trans-shipment, brokering, transport, transfer, stockpiling or use of WMDs and their means of delivery.

Proliferators and their networks will therefore evaluate vulnerabilities in jurisdictions with poor or weak financial regulations or compliance and target financial institutions to enable them to procure items.

Therefore, both export control mechanisms, aimed at countering WMD proliferation by closely monitoring the movement of proliferation-sensitive items, and financial establishments, which not only facilitate payment processing for commercial transactions but also ensure the seamless transfer of goods through trade finance and insurance services, are interconnected in their efforts to counter proliferation financing.

Proliferation schemes are designed based on in-depth knowledge of the jurisdictions' structural and sectoral vulnerabilities. WMD proliferators are able to evaluate the chances of procuring goods by exploiting, for instance, looser police, customs or export controls applied in transshipment hubs and free trade zones to conceal the final destination and detach end-user proliferators from the commercial transactions. These malicious actors also target

jurisdictions with permissive corporate service environments characterized by weak financial controls or less developed compliance culture so that they may establish front and shell companies to obfuscate their identities and hinder investigations.

The Royal United Services Institute proposes a distinction between forms of proliferation financing. The above paragraph, involving the ‘actual or attempted financing of proliferation-sensitive goods and technologies’, would be a form of direct PF. In contrast, activities that could ‘substantively contribute to a state or non-state actor’s WMD programme’, such as cyber-heists and IT workers overseas, would be indirect PF. Gibraltar, as an international finance centre (IFC) and a services-based economy, is exposed to both these forms of PF to varying degrees.

At its core, PF focuses on the risks associated with financial products and services which are directly linked to the trade in proliferation-sensitive items and procurement of proliferation-sensitive technologies. As the FATF has noted in a recent report on sanctions evasions typologies, there are many legitimate factors that lessen the potential that PF threat actors might exploit vulnerabilities, including geographical distance, a lack of trade or diplomatic relations, and no prior PF cases. Nonetheless, ‘because PF threat actors thrive on exploiting potential blind spots in the international financial system’, and as new technologies emerge and geopolitical circumstances change, Gibraltar remains keenly aware of risks it may face in the present and future.

Definition

To better understand what proliferation financing is, it needs to be defined. A lack of an internationally agreed-upon definition or details on the type of domestic legislation countries are expected to implement creates a gap in how individual states interpret the provisions under the United Nations Security Council Resolution (UNSCR) 1540. To cover this gap, the Financial Action Task Force (FATF), drafted a working definition to assist countries in better interpreting the provisions of Resolution 1540.

Therefore, for the purpose of this NRA, the definition of the financing of proliferation refers to:

“The risk of raising, moving, or making available funds, other assets or other economic resources, or financing, in whole or in part, to persons or entities for purposes of WMD proliferation, including the proliferation of their means of delivery or related materials (including both dual-use technologies and dual-use goods for non-legitimate purposes).”

Scope

The complexity and transnational nature of proliferation activities and proliferation financing spans the globe. However, this NRA's scope covers activities which have a Gibraltar nexus that potentially threaten Gibraltar's financial system and/or national security. Working with international partners, and understanding international dynamics, nonetheless remains key to interdicting proliferation financing networks. These activities can either directly or indirectly finance an actor's procurement of WMD technology.

Methodology

This assessment follows the FATF methodology, where PF risk is a function of the following:

Threat refers to designated persons and entities that have previously caused, or have the potential to cause, the evasion, breach or exploitation of a failure to implement PF targeted financial sanctions (PF-TFS) in the past, present or future. Such threat may also be caused by those persons or entities acting for or on behalf of designated persons or entities. Intent and

capability are both implicit in this definition. It can be an actual or a potential threat. Not all threats present the same risk level to all countries and private sector firms.

Vulnerability refers to matters that can be exploited by the threat or that may support or facilitate the breach, non-implementation or evasion of PF-TFS. These vulnerabilities may include weaknesses in our laws or regulations that comprise our counter proliferation financing regime, or contextual features that may provide opportunities for designated persons and entities to raise or move funds or other assets. More broadly, where threats often originate externally, vulnerability is concerned with internal structures. For private sector firms, vulnerabilities may include features of a particular sector, a financial product or type of service that make them attractive for a person or entity engaged in the breach, non-implementation or evasion of PF-TFS.

Consequence refers to the outcome where funds or assets are made available to designated persons and entities, which could ultimately allow them, for instance, to source the required materials, items, or systems for developing and maintaining illicit nuclear, chemical or biological weapon systems (or their means of delivery), or where frozen assets of designated persons or entities would be used without authorisation for proliferation financing. A breach, non-implementation or evasion of PF-TFS may also cause reputational damages to Gibraltar, relevant sector(s) or private sector firms, and punitive measures such as sanction designations by the UN and/or competent authorities. Ultimately, the consequence of proliferation financing, i.e. the threat of use or the use of a weapon of mass destruction, is more severe than that of ML or other financial crimes and is more similar to the potential loss of life associated with the consequences of TF.

Risk is a function of threat, vulnerability, and consequence. It represents a summary judgment, considering the effect of mitigating measures, including regulation, supervision, and enforcement.

Further in line with the prior assessments, the assessment is based on a review of public and private sector publications, government datasets, and analyses. Data collected are current as of January 31, 2024.

These sources include:

Data collected via the Joint Coordination Intelligence Group (JCIG) membership which includes but not limited to; GFIU data, HMC data on imports and exports controls, GFSC data, Borders and Coastguard immigration data, Gibraltar Port Authority and Gibraltar Maritime Administration datasets on vessels. No MLA requests have been received in connection with PF, nor have any STRs been submitted with a PF concern up to June 2025.

Risk Assessment

In October 2020, the FATF revised Recommendation 1 and its Interpretive Note (R.1 and INR.1) to require countries and private sector entities to identify, assess, understand and mitigate their proliferation financing risks (PF risk). In the context of R.1 and of this Guidance, proliferation financing risk refers strictly and only to the potential breach, non-implementation or evasion of the targeted financial sanctions (TFS) obligations referred to in Recommendation 7.3.

In addition to obligations for countries, the revised FATF Standards require private sector entities to have in place processes to identify, assess, monitor, manage and mitigate proliferation financing risks. Private sector entities may do so within the framework of their existing targeted financial sanctions and/or compliance programmes and are not expected to establish duplicative processes for proliferation financing risk assessment or mitigation.

Targeted financial sanctions

Sanctions are one of two coercive measures under Chapter VII of the UN Charter, the other being military force. Article 41 of the Charter mentions a variety of measures available to the UN Security Council (UNSC), including “complete or partial interruption of economic relations and of rail, sea, air, postal, telegraphic, radio, and other means of communication, and the severance of diplomatic relations.” Sanction circumvention and evasion activities are often enabled by states with weak or lax implementation and/or enforcement of the UNSCRs including global export controls measures related to WMDs to prevent proliferation to non-state actors under UNSCR 1540.

The two countries directly targeted by UN sanctions to limit their proliferation activities are the DPRK and Iran. Sanctions were imposed on the DPRK after UNSCR 1718, passed in 2006 in response to the country’s first nuclear test. Provisions include bans on materials, equipment, goods and technology that could contribute to their proliferation efforts. UN sanctions against Iran also began in 2006, in response to the country’s failure to cease uranium enrichment activities. They formally expired in 2023 following the Joint Comprehensive Plan of Action, but the US, EU and UK have all subsequently re-applied unilateral sanctions.

Gibraltar’s measures for the effective, timely implementation of targeted financial sanctions (TFS) relating to PF are robust. As a jurisdiction, Gibraltar applies UN, UK, and EU sanctions (with UK designations given preference over EU ones in the event of any conflict of interest).

Domestic legislative frameworks are comprehensive and allow for the rapid implementation of sanctions. The Weapons of Mass Destruction Act (2004) outlines offences relevant to the development, production, acquisition, retention and transfer of WMDs. Gibraltar adheres to the legislative requirements established in the Chemical Weapons (Sanctions) (Overseas Territories) Order 2018, as well as the DPRK Sanction Order 2018. The latter specifically identifies ‘making funds or economic resources to a designated person’, ‘failing to comply with reporting obligations’, and ‘activities that circumvent an asset freeze’ as offences.

New sanctions designations from the UN and UK are sent to reporting entities via the GFIU’s reporting mechanism, which allows them to have immediate oversight of any impact on their clients and client nexus. The Sanctions Act 2019 delimits the competent authority’s powers (the office of Chief Minister) relating to the designation of persons and ships. As Gibraltar is not a sovereign state, and foreign relations remain a prerogative of the UK, the Chief Minister cannot unilaterally designate persons or ships but can inform the UN to secure the making of a designation in coordination with the UK Foreign, Commonwealth and Development Office.

Considering the unique circumstances that apply to Gibraltar as a British Overseas Territory, the jurisdiction is prepared from legislative and practical perspectives for the rapid implementation of TFS. Although not directly PF related, the seizure of a vessel in 2019 by Gibraltar authorities in collaboration with the UK is testament to the jurisdiction’s ability to play a pivotal, proactive role in combating sanctions evasion.

UNSC Resolution 1540

The UNSC adopted resolution 1540 (2004) under Chapter VII of the UN Charter. UNSCR 1540 calls on all UN member states to enact legally binding measures for criminalising the proliferation of WMDs. The resolution affirms that the proliferation of nuclear, chemical and biological weapons and their means of delivery constitutes a threat to international peace and security. The resolution obliges States, inter alia, to refrain from supporting by any means non-state actors (NSAs) from developing, acquiring, manufacturing, possessing,

transporting, transferring or using nuclear, chemical or biological weapons and their means of delivery.

UNSCR 1540 encompasses three main obligations:

- All States are prohibited from providing any form of support to non-state actors seeking to acquire weapons of mass destruction, related materials, or their means of delivery.
- All States must adopt and enforce laws criminalising the possession and acquisition of such items by non-state actors, as well as efforts to assist or finance their acquisition.
- All States must adopt and enforce domestic controls over nuclear, chemical, and biological weapons, their means of delivery, and related materials, in order to prevent their proliferation.

Gibraltar endorses the implementation of UNSCR 1540 as a crucial measure to mitigate the proliferation of WMDs and enhance global security through its legal framework. Its aims and objectives were reinforced by UNSCR 2325 (2016), which was the first resolution to explicitly mention 'proliferation financing', and UNSCR 2663 (2022), which upheld and encouraged continued compliance with Resolution 1540.

State Actors

DPRK

The Democratic People's Republic of Korea (DPRK) continues to violate Security Council resolutions through various techniques in an attempt to circumvent UNSC resolutions. Although it has not conducted any nuclear test since 2017, it has reaffirmed its commitment to retaining and developing nuclear and ballistic missile programmes. The DPRK continues to challenge the UN sanctions regime to fund its WMD program and has diversified its strategy via various means, including reportedly using cyberattacks as a source of income. According to the UN Panel of Experts reports the trends include 'targeting defence companies and supply chains and, increasingly, sharing infrastructure and tools. Despite being the most sanctioned state, the DPRK has increased its WMD capacity and technology in recent years.

Iran

The continued lack of progress with the Joint Comprehensive Plan of Action (JCPOA), which was concluded in 2015 by China, France, Germany, Russia, the United Kingdom, the United States and the European Union with the Islamic Republic of Iran, to achieve shared non-proliferation and regional security objectives, appears to have grown increasingly unlikely given current geopolitical dynamics. Despite the Israeli-American offensive in June 2025 seeking to negate Iran's alleged capacity to develop a nuclear weapon, intelligence reports remain unclear regarding its effectiveness, and outcomes remain uncertain for Iran's proliferation regime.

Russia

Russia's ongoing war against Ukraine has significantly affected its military hardware, which has relied heavily on foreign components. To address the losses sustained in battle, Russia has sought new procurement relationships and turned to both the DPRK and the Islamic Republic of Iran. Consequently, Russia is often referred to as a 'state of proliferation concern'. Additionally, Russia's veto in the UN Security Council, to adopt a resolution that would extend the mandate of the UN Panel of Experts on the DPRK, will hinder a comprehensive understanding of the DPRK's WMD program development and the associated financing typologies. Despite this, the UNSCRs against the DPRK remain in effect.

Non-state Actors

The term ‘non-state actors’ can be seen as the attempt of terrorist groups, such as Al-Qaeda and the Islamic State (or Daesh), to acquire WMD capabilities. However, it is essential to understand the term in order to have greater scope for identifying these actors. State actors such as Iran and the DPRK have also involved the use of non-state actors as intermediaries to access materials, components and technology to assist in their WMD program. Whilst UNSCR 1540 was designed to limit the ability of terrorist groups to acquire and deploy nuclear, chemical or biological weapons, the broad range of actors involved under the term ‘non-state actors’ presents a challenge. Focusing on the motivation of these non-state actors, which could be ideological or economic, provides us with better detection opportunities.

Wittingly or unwittingly supplying WMD programmes is also an essential element of this. Manufacturers, exporters, distributors, insurers, financial institutions, and transporters may breach sanctions by either wittingly or unwittingly being involved with state actors. Therefore, it is essential that the scope of understanding of proliferation financing is broadened to capture any involvement by a large range of actors. This includes the exportation of dual-use goods.

Legislation

Frameworks to combat proliferation financing rely on three interlinked layers of obligation: international legal mandates established by the United Nations Security Council, recommendations from the Financial Action Task Force, and domestic legislation. These layers collectively impose requirements that influence the risk management practices of reporting entities in the financial sector.

Gibraltar has a strong legal framework that criminalises proliferation financing. These include offences relevant to the development, production, acquisition, retention and transfer of nuclear, biological and chemical weapons, pursuant to the Weapons of Mass Destruction Act 2004. As a British Overseas Territory, Gibraltar is also required to adhere to the legislative requirements set out under the Chemical Weapons (Sanctions) (Overseas Territories) Order 2018.

Domestic legislation also applies certain measures to give effect to decisions under Council Regulations (EU) which relates to the Democratic People’s Republic of Korea (DPRK) Sanction Order 2018. This order repeals the DPRK Sanction Order 2016 and creates offences which include: making funds or economic resources available to a designated person (except where an exemption applies or under licence), dealing with funds or economic resources that must be frozen (except where an exemption applies or under licence), and failing to comply with reporting obligations, activities that circumvent an asset freeze, and breaches of licensing conditions.

In addition, since February 2021, Gibraltar adopted a definition of proliferation financing in section 38A of the Terrorism Act 2018 and instituted related offences and further changes to POCA as a result of this.

Regulatory Measures

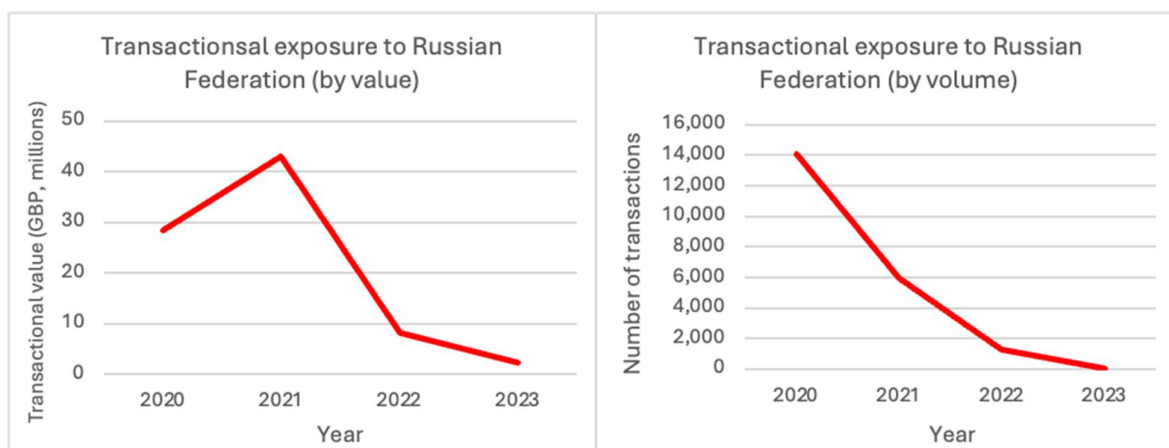
Relevant financial businesses operating in or from within Gibraltar are subject to authorisation and supervision by the Gibraltar Financial Services Commission (GFSC). As part of its supervisory programme, the GFSC ensures that each institution has sufficient controls in place to manage and mitigate the risk of its services being used to facilitate money laundering (ML), terrorist financing (TF) and PF. The remit of the GFSC’s supervisory approach was extended to include PF (in addition to ML and TF) in February 2021. The GFSC

is therefore relatively advanced in supervising its regulated entities' counter-proliferation financing measures.

In practice, the GFSC assesses the veracity of a regulated entity's counter-proliferation financing controls by way of its on-site and desk-based review programmes. Below is a non-exhaustive list of key considerations that the GFSC assesses and verifies when undertaking its supervisory assessments:

- a. The inclusion of a robust assessment of PF-related risks within an entity's enterprise-wide risk assessment;
- b. The awareness of key personnel in relation to PF risks, as well as the associated red flags and typologies;
- c. The inclusion of PF controls within an entity's policies, procedures and risk mitigation measures; and
- d. Adherence to PF-related targeted financial sanctions.

In cases of non-compliance, the GFSC has a range of effective, proportionate and dissuasive sanctioning measures available to it. An assessment of an entity's controls in relation to the combating of ML, TF and PF also forms a key part of the GFSC's authorisations process. Since 2021, the GFSC has noted a substantial improvement in the understanding and awareness of PF risks, red flags and typologies amongst its regulated entities. The number of findings that relate to an entity's documented procedures extending to counter-proliferation financing measures (in addition to ML and TF) has also significantly decreased since 2021.



As set out within the graphs above, the level of exposure to the Russian Federation has also decreased significantly year-on-year since 2020 (in terms of both transactional volume and value).

Cooperation and Coordination – The Joint Coordinating Intelligence Group

FATF Recommendation 2 states that countries should establish appropriate inter-agency frameworks for co-operation and co-ordination with respect to combating money laundering, terrorist financing and the financing of proliferation. These may be a single framework or different frameworks for ML, TF and PF respectively.

Consequently, the GFIU established the Joint Coordination Intelligence Group (JCIG) for Counter Proliferation Financing. This multi-agency forum is composed of; the Gibraltar Financial Intelligence Unit, Gibraltar Financial Services Commission, Royal Gibraltar Police, HM Customs, Borders and Coastguard Agency, Gibraltar Port Authority, Government Law Office, Gibraltar Maritime Authority and Office of Fair Trading. By exchanging intelligence on

suspected proliferators, networks, vessels, sanctioned entities, and other assets, the JCIG facilitates strategic coordination to detect, prevent, and disrupt proliferation activities. Inter-agency collaboration and intelligence sharing is fundamental to understanding current and emerging typologies, particularly as no PF STRs have been submitted to the GFIU to date.

Exports Controls and Dual-use Goods

The European Commission defines dual-use goods as a 'product, technology and software which can be used for civilian and military applications and or can contribute to the increase of WMD'. Global rapid technological advances are continuously increasing the risk of biological, chemical and nuclear attacks⁹. Therefore, export control measures become an important tool to prevent, deter and halt the proliferation of WMDs. Export of dual-use goods means the transfer of items or goods from the exportation state to another state. Gibraltar's legislative framework on export control measures requires any person who wishes to conduct any activity in the exportation of dual-use goods will be required to obtain a licence prior to conduct any such activities.

Gibraltar is not a manufacturing economy and has no industrial capability to produce dual-use goods or military items. As it is located at the entrance to the Mediterranean, however, there may be scope for the re-export of these goods. Moreover, the global trade in dual-use goods implicates companies that may or may not be present in jurisdictions where trade is occurring.

The existing complements of the HMC EPU (documentary checks) and the HMC Controls Unit (physical examination of goods on importation and exportation), who work closely together, are in conjunction able to provide the resources necessary to monitor the movements of Dual Use goods through the alert system incorporated into the customs database (ASYCUDA) and its programmed selectivity criteria. Equally, the FIT, with their two extra officers and the training provided by the GFIU through presentations and the e-Nexus platform, dedicate time to analyse the data collated from the movements of such goods being imported, exported or transported in transit through Gibraltar. Any intelligence gathered will then be forwarded to the GFIU.

CASE STUDY: Outreach & Engagement

Since 2020, there have been fundamental changes to legislative and regulatory frameworks that support counter proliferation efforts. These have been strengthened by an intense outreach and engagement programme that covers proliferation financing through Project Nexus, e-Nexus and comprehensive Guidance Notes to enhance the understanding of the complexities and challenges in identifying proliferation financing techniques, red flags and typologies. A recent survey conducted by the GFIU for both public and private sector partners concluded that there is a high level of awareness and understanding proliferation financing and the difference between proliferation financing related sanctions and terrorist financing related sanctions.

Exploitation of the Maritime and Shipping Sector

In Gibraltar, where the maritime and shipping sector, and port facilities serve as an essential hub for transiting ships and bunkering services, proliferation networks may pose a risk. These networks often exploit the commercial supply chain to evade detection and finance the procurement of restricted materials, often using shipping companies and vessels. Gibraltar's strategic position at the entrance to the Mediterranean makes it potentially

⁹ Council - Report of 11 December 2008 on the implementation of the European Security Strategy – Providing security in a changing world, S407/08 [2008], p.3.

vulnerable to activities such as sanctions evasion and export control violations, with front and shell companies masking the identities and activities of threat actors.

Addressing these threats requires not only maritime-focused strategies but also strong land-based efforts. The origins of these threats, the impacts felt onshore, and the need for enforcement and prevention all highlight the importance of collaboration between land-based and maritime entities. This combined approach strengthens Gibraltar's ability to counteract such risks effectively and protect its role as a key maritime gateway.

The maritime sector remains essential to the infrastructure of PF networks. For states under comprehensive sanctions, illicit import-export activities frequently involve vessels and deceptive practices like vessel identity laundering, flag-hopping, and automatic identification systems (AIS) spoofing to avoid detection by relevant authorities. These methods complicate oversight and emphasise the need for strong compliance frameworks in Gibraltar's maritime sector.

State actors engaged in sanctions evasion have developed "shadow fleets" that use complex structures, such as flags of convenience and intricate ownership webs, to mask the origins and destinations of their cargo. These fleets employ various tactics to avoid detection, including ship to ship transfers, disabling or manipulating AIS systems, providing false location data, and using other deceptive or illegal measures. With many of these vessels being older and often poorly maintained, these shadow fleets not only enhance the financial resources of these states but also introduce substantial risks to environmental protection, maritime safety, and regional security by operating with minimal regulatory oversight.

Firms operating in trade finance should also be aware of the potential misuse of trade finance instruments in proliferation-related activities. In addition to Gibraltar's regulatory requirements, firms should consult international resources like the FATF PF Risk Assessment Guidance and FATF Guidance on Trade-Based Money Laundering, or the RUSI Institutional Proliferation Finance Risk Assessment Guide, which provide strategies to detect and mitigate these threats.

Strengthening compliance measures and raising awareness of PF typologies in Gibraltar's maritime sector will be crucial in countering these complex threats and safeguarding Gibraltar's strategic role as a maritime gateway against exploitation by proliferation networks.

Emerging Trends

Proliferation networks continue to adapt their methods to circumvent sanctions and evade detection. Proliferators are increasingly embracing technological advancements. Alternative monetary products, such as emerging financial technologies, have created novel avenues for state actors to generate funds for their WMD programmes. The exploitation of these financial technologies through mining and theft of virtual asset exchanges facilitates the transfer of illicit proceeds and avoids the scrutiny of regulators. Enhancing cybersecurity infrastructures around VASPs will mitigate the risks associated with criminal cyber activities. In its search for military components and materials to support its war against Ukraine, Russia has recently redefined its relationship with the DPRK and Iran, which increases potential proliferation threats.

The DPRK's deployment of IT workers abroad poses significant challenges to firms employing freelance or remote IT professionals. These state-sponsored operatives fraudulently secure employment with companies in the UK, US, and other countries, generating substantial revenue for the DPRK regime. This income, which is often funnelled into the DPRK's WMD and ballistic missile programs, poses a serious international security risk and is in violation of UNSCRs prohibiting North Korean citizens working abroad, namely UNSCR 2397 (2017). DPRK IT workers employ sophisticated tactics, including identity fraud,

VPNs to mask their true location, and leveraging non-DPRK enablers to provide accounts, infrastructure, and identity verification. They use stolen or synthetic identities, falsified documents, and even AI tools such as deep fakes to deceive employers and hiring platforms.

Operating primarily from Russia, China, and other regions, these IT workers present themselves as remote freelancers, skilled in software development, graphic design, and animation. Their activities are further obscured through front companies, fake websites, and manipulated online personas. They also exploit freelance platforms to gain access to sensitive data, plant malware, and conduct social engineering schemes, putting organisations at risk of data breaches, intellectual property theft, and legal consequences for violating sanctions. The global reach of the internet means that Gibraltar companies are plausibly as much at risk as other jurisdictions. The DPRK's targeting of cryptocurrency companies might pose a particular risk to Gibraltar's burgeoning VASP sector.

The DPRK regime retains up to 90% of the earnings from these workers, which according to reports total hundreds of millions of dollars annually, directly funding prohibited military programs. To mitigate this threat, the UK's Office of Financial Sanctions Implementation (OFSI) has issued advisory notices to help entities conduct enhance due diligence¹⁰.

Firms are urged to adopt layered defences, including stringent identity verification, monitoring for suspicious activity, and staying informed about evolving tactics. Regular audits and continuous vigilance are essential to counter this growing challenge and ensure compliance with international sanctions. Nonetheless there are no indications or known incidents of this type associated with or occurring within Gibraltar.

Virtual Asset Service Providers and Cyber-enabled proliferation financing

In 2023, the GFIU conducted a research paper that aimed to analyse key elements of the DPRK's cyber capabilities and further the understanding of how state-actors launder the illicit proceeds exploiting global financial ecosystems to support its nuclear and ballistic missile program. Using various sources including open-source data, think tank research papers, academic literature and case studies, the paper provides an analysis of the DPRK's cyber strategy, the threat actors and techniques, tactics and procedures attributed to these actors. It explored ransomware, cyber heists and the theft of virtual assets from crypto exchanges, mixers and blockchain bridges. It highlighted the techniques and tactics employed by the DPRK to exploit cyber systems to generate illicit revenue and launder the proceeds to fund its nuclear and ballistic missile program. It concluded that the risk of cyber-enabled proliferation financing is increasingly complex in nature with a fundamental link between the DPRK's cyber strategy, cyber threat actors, and its illicit cyber operations. Despite this link, our understanding of the impact on financial institutions remains limited and underdeveloped. The impact may be larger than expected and could be due to underreporting of cyber-attacks due to reputational risks. This situation poses new challenges for financial institutions, as the potential loss of data and funds can have severe and far-reaching consequences.

The UN Panel of Experts Reports on the DPRK highlight the threats and vulnerabilities associated with both virtual assets and VASPs. The embezzlement of virtual assets continues to be a key means through which the DPRK obtains funds for the purposes of furthering its WMD programmes. This is achieved primarily through cybercrime-related theft, targeting institutions (including VASPs) operating within a wide array of jurisdictions. It is estimated

¹⁰

https://assets.publishing.service.gov.uk/media/66e2ec410d913026165c3d91/OFSI_Advisory_on_North_Korean_IT_Workers.pdf

that the equivalent of \$2.3 billion in virtual assets has been the stolen by the DPRK from 2017 to 2022 (with an additional approximate \$750 million identified in 2023 which is in the process of being investigated). In early 2025, a DPRK-linked group stole approximately \$1.5bn in one attack. The final UN Panel of Experts Report published in March 2024 refers to a statement made by a Member State official, assessing that the malicious cyberactivity of the DPRK accounts for approximately half of the funding contributed towards its missile programme.

VASPs operating in or from within Gibraltar are subject to authorisation and supervision by the GFSC. VASPs are required to seek authorisation under either the Distributed Ledger Technology (DLT) framework, or registration under the VASP framework (collectively referred to as the VASP sector). Both regimes are subject to the same level of supervision for the purposes of combatting ML, TF and PF as all other GFSC-regulated sectors. The regulatory regime that each VASP is subject to is dependent on the nature of its underlying products and services. In the case of the DLT framework, providers are also subject to additional sets of regulatory requirements, including those related to maintaining a high standard of cybersecurity controls. This acts to mitigate the risk of those providers being targeted by the DPRK's illicit cyber actors.

The standard of compliance maintained by the VASP sector is generally satisfactory, with an observed decrease in the number/significance of AML/CFT/CPF-related deficiencies identified by the GFSC by way of its on-site inspections. From 2020 to 2023, the VASP sector has also been identified as the second highest reporting sector in terms of SARs to the GFIU. It is important to note, however, that no SARs have been submitted in relation to PF (which is considered commensurate with the jurisdiction's overall PF risk profile). The VASP sector in particular, is also assessed by the GFSC as having a robust understanding of PF, together with the associated risks, red flags and typologies.

As with all other regulated sectors, the GFSC has a wide range of proportionate and dissuasive sanctioning powers available to it in cases of non-compliance with the relevant legislative and regulatory requirements. Since the inception of the DLT & VASP frameworks, the GFSC has taken supervisory action against a number of regulated VASPs as a result of identified AML/CFT/CPF-related deficiencies.

The threat is low but instances of proliferation financing within Gibraltar's finance centre cannot be discarded.

11 Tax Crime Risk

11.1 Introduction

The interactions between money laundering, tax exchange and tax compliance are extensive. Money laundering and tax evasion are often interconnected activities. Criminals engaged in money laundering may utilise tax evasion arrangements and schemes to hide illicit funds and avoid corresponding tax obligations. They exploit loopholes in tax systems and utilise offshore tax havens or complex corporate structures to obscure the true ownership and control of assets. Strengthening the exchange of tax information and associated compliance helps combat this by promoting transparency and cooperation between jurisdictions; making it harder for criminals to benefit from the exploitation of a lack of cooperation.

Regulated entities play a critical role in facilitating or preventing money laundering and tax evasion. Inadequate compliance measures can inadvertently aid criminals in moving and legitimising illicit funds. In contrast, strong compliance measures, including rigorous customer due diligence, robust transaction monitoring systems and reporting of suspicious activities are essential for detecting and preventing these. Technological advancements have introduced new challenges in combating money laundering and tax evasion. Digital assets, like cryptocurrencies, provide criminals an added layer of anonymity for exploitation. Regulatory efforts and the introduction of stricter regulations seek to promote transparency in this space to address these challenges.

International cooperation and information sharing are crucial for combating money laundering and tax evasion effectively. Financial intelligence units, tax authorities and other regulatory bodies are vital in coordinating efforts to detect and prevent financial crimes. Global initiatives provide a set of standards, guidance and rules for tax information exchange, anti-money laundering and counter-terrorism financing measures; all of which facilitate global cooperation and ensure consistent compliance frameworks. In understanding this interaction, governments, regulatory bodies, and financial institutions enhance their tools against financial crimes ensuring tax compliance and safeguarding the integrity of the global financial system.

11.2 Domestic framework

The Income Tax Office in Gibraltar is responsible for the administration, assessment and collection of personal income tax and corporate income tax under the Income Tax Act 2010 and its corresponding subsidiary legislation.

In addition to the above, the Income Tax Office also discharges the competent authority function for the exchange of tax information and administrative cooperation under Gibraltar's multilateral and bilateral international tax agreements.

The Income Tax Office exchanges intelligence and information with law enforcement agencies and regulatory bodies in Gibraltar, including the Economic Crime Unit of the Royal Gibraltar Police; the Investigation Branch of HM Customs, the Financial Intelligence Unit and the Gambling Division under specific Memorandums of Understanding and legal gateways enabling this level of domestic cooperation. The Gibraltar tax authorities will also shortly be concluding a Memorandum of Understanding with the Gibraltar Financial Services Commission. This sharing of information and intelligence seeks to aid in identifying and mitigating the risks associated from tax-related offences and other criminal conduct including money laundering and financing of terrorism.

The Gibraltar tax authorities support the work of these other authorities from a tax perspective through its ability to exchange and share information relevant for the purposes of carrying on their respective functions. This extends to include the following:

- domestic tax compliance activities to ensure all taxpayers pay the proper amount of tax based on statutory provisions; and
- work under the various international tax agreements, to the extent that the information exchanged is relevant to the functions of other authorities.

The collaboration and cooperation between the tax authorities and those agencies responsible for policing money laundering and the financing of terrorism includes:

(i) The administration of domestic income tax rules

The Income Tax Office in Gibraltar may investigate cases of potential tax crimes (although almost all are civil matters) focusing on Gibraltar taxpayers intentionally looking to evade paying the correct amount of income tax by not making a full and complete declaration of income on their tax returns. The Gibraltar authorities would refer any instances of serious fraud to the Economic Crime Unit of the Royal Gibraltar Police and a determination made if a joint investigation should go ahead and whether potential tax evasion would be a predicate offence for money laundering.

(ii) The exchange of information

As competent authority for Gibraltar, the Income Tax Office are the recipient of requests for information that are foreseeably relevant for a tax investigation/enquiry in the taxpayer's jurisdiction of tax residence.

Gibraltar is committed to continuing to deter tax crime through transparency, information sharing and effective tax cooperation. Domestic initiatives such as a program of tracing through of tax information requests received by the tax authorities to intelligence available to the Gibraltar Financial Intelligence Unit and/or the Economic Crime Unit of the Royal Gibraltar Police is being pursued to determine and evaluate the effectiveness of international collaboration.

11.3 International tax cooperation, transparency and exchange of information

Up until its date of exit from the European Union on 31 December 2020, Gibraltar fully transposed and implemented applicable EU directives in relation to administrative cooperation for transparency and the exchange of information for tax purposes. Following its exit from the EU, Gibraltar has ensured continued compliance with global standards of transparency and exchange of information through equivalent instruments as a member of the OECD's Global Forum and the Inclusive Framework on the Base Erosion and Profit Shifting Action (BEPS).

These Directives on Administrative Cooperation (DACs) covered various forms of exchange of information for tax purposes as summarised below.

EU Directive (DAC)	Description
Council Directive 2011/16/EU (DAC1)	Exchange of information on request. Automatic exchange of information on specific categories of income. Spontaneous notifications to other participating jurisdictions.
Council Directive 2014/107/EU (DAC2)	Automatic exchange of financial account information.
Council Directive 2015/2376/EU (DAC3)	Exchange of information in relation to advance cross-border rulings and advance pricing arrangements.
Council Directive 2016/881/EU (DAC4)	Automatic exchange of Country-by-Country reports.
Council Directive 2018/822/EU (DAC6)	Automatic exchange of information on reportable cross-border arrangements.

TABLE 36 - DIRECTIVES ON ADMINISTRATIVE COOPERATION (DACs)

Whilst these directives are no longer operable, Gibraltar continues exchanging information under equivalent instruments including: the OECD and Council of Europe's Multilateral Convention on Mutual Administrative Assistance in Tax Matters; Tax Information Exchange Agreements (TIEAs); and other bilateral tax agreements.

Gibraltar has collaborated with the OECD Global Forum on Transparency and Exchange of Information for Tax Purposes in respect of tax information exchange since 2002 and has participated in all of the Global Forum's annual assessments since 2006. It became a member of the Global Forum in 2009 after concluding its first Tax Information Exchange Agreement (TIEA) with the United States, reiterating its firm commitment to uphold the international standard for transparency and exchange of information for tax purposes. Since then, it has built up a network of exchange of information agreements including with key trading partners. Gibraltar remains an active participant in the OECD's Global Forum on Transparency and Exchange of Information for Tax Purposes.

Gibraltar has concluded further bilateral tax agreements allowing for a range of exchange of information and administrative cooperation, including:

- 27 TIEAs with other jurisdictions:

Australia (26 July 2010)	Italy (12 June 2015)
Austria (1 May 2010)	Malta (1 April 2012)
Belgium (17 June 2014)	Mexico (27 August 2014)
Denmark (13 February 2010)	Netherlands (1 December 2011)
Faroese (8 June 2011)	New Zealand (13 May 2011)
Finland (6 May 2010)	Norway (8 September 2010)
France (9 December 2010)	Poland (5 December 2013)
Germany (4 November 2010)	Portugal (24 April 2011)
Greenland (23 January 2010)	South Africa (21 July 2013)
Guernsey (12 March 2014)	Sweden (3 July 2010)
Iceland (18 April 2012)	Turkey (15 February 2018)
India (11 March 2013)	United Kingdom (15 December 2010)
Ireland (25 May 2010)	United States (22 December 2009)
Isle of Man (5 February 2020)	
- an International Agreement on Taxation and the Protection of Financial Interests between the Kingdom of Spain and the United Kingdom of Great Britain and Northern Ireland regarding Gibraltar on 4 March 2019, which entered into force on 4 March 2021; and
- a comprehensive Double Taxation Agreement with the United Kingdom on 15 October 2019, based on the OECD's Model Tax Convention on Income and on Capital and which entered into force on 24 March 2020.

Gibraltar's TIEAs are all OECD Global Forum Model Agreements on the Exchange of Information in Tax Matters.

Gibraltar is also a participating jurisdiction in the OECD's Multilateral Convention on Mutual Administrative Assistance in Tax Matters since 1 March 2014. This convention is the most comprehensive multilateral instrument available for all forms of tax cooperation to tackle evasion and avoidance and includes 147 jurisdictions including all G20, BRIIC and OECD countries, major financial centres, and several developing countries. The OECD Convention

provides a more comprehensive and efficient exchange framework than bilateral TIEAs and is now the principal method of information sharing between jurisdictions.

In total, Gibraltar has 160 exchange of information agreements in force with other jurisdictions and an exchange of information relationship in force with 134 jurisdictions, all of which enable the exchange of information in respect of both criminal and civil tax matters.

Regarding automatic exchange of information in taxation, Gibraltar entered into a Model 1 IGA reciprocal agreement with the United States in November 2013, enabling the implementation of their Foreign Account Tax Compliance Act (FATCA). Gibraltar exchanges information under this agreement annually, having begun these exchanges in 2014. At around the same time, Gibraltar was among the “early adopter” group of jurisdictions that committed to undertaking first exchanges under the OECD’s Common Reporting Standard (CRS) in 2017. The CRS, also known as the Standard for Automatic Exchange of Financial Account Information in Tax Matters, requires financial institutions in participating jurisdictions to provide information to their domestic tax authorities on any financial accounts held by persons that are tax resident in foreign participating jurisdictions. The domestic tax authorities must then automatically pass on that information to the tax authorities in the foreign jurisdiction annually. Its principal goal is to provide tax authorities with intelligence concerning financial accounts held by their taxpayers in foreign jurisdictions, enabling them to carry out compliance activities to determine any tax risks. The domestic adoption of the Standard for Automatic Exchange of Financial Account Information in Tax Matters provides for robust due diligence and reasonable measures for the purposes of identifying tax residence subject to an annual declaration, including an exhaustive list of procedures and requirements for supporting evidence.

As part of its expansion of CRS-related exchanges, Gibraltar concluded bilateral agreements consistent with the CRS Bilateral Competent Authority Agreement with Guernsey and Isle of Man under the relevant articles allowing for automatic exchanges within their respective TIEAs.

The Global Forum’s Assessment Panel for the Transparency and Exchange of information for Tax Purposes has consistently rated Gibraltar ‘Largely Compliant’ in its effectiveness review of the jurisdiction’s exchange of information under their terms of reference. Gibraltar is always willing to engage in discussions with other countries to develop bilateral relations. These bilateral agreements make it possible, via information exchange requests, to provide assistance for targeted tax-related requests.

Reaffirming its international efforts to combat international tax evasion, Gibraltar joined the OECD/G20 Base Erosion and Profit Shifting (BEPS) Project in 2019. As an Inclusive Framework Member, Gibraltar has successfully adopted all mandatory and minimum standards: Action 5: Harmful Tax Practices, Action 6: Prevention of tax treaty abuse, Action 13: Country-by-Country Reporting and Action 14: Mutual Agreement Procedure.

Gibraltar fully implements Action 5 relating to harmful tax practices on the basis that no such practices exist in Gibraltar. It is also fully compliant on Actions 6 and 14 since its Double Taxation Agreement with the United Kingdom transposes the relevant model provisions designed by the BEPS project to prevent treaty abuse and includes the relevant article allowing for a Mutual Agreement Procedure as an effective and efficient dispute resolution mechanism.

Gibraltar introduced its Country-by-Country regime in 2017 following transposition of the applicable EU directive and then as part of Article 13 of the OECD’s BEPS. Under this regime,

a Gibraltar tax resident company, that is the ultimate parent entity of a multinational group with consolidated revenue of at least €750 million, must, in predefined circumstances, file a report containing financial information including revenue, profit/(loss), tax paid, number of employees and assets with regards to each jurisdiction in which the group operates. This report also shows each constituent entity of the group, their jurisdiction of tax residence and the nature of the core business activity. Constituent entities in Gibraltar of such groups have an obligation to file a notification, also in predefined circumstances, declaring the jurisdiction of tax residence of the ultimate parent entity and filing of the report. The OECD's Co-ordinating Body Secretariat confirmed the effectiveness of Gibraltar's exchanges and its compliance with Action 14.

As part of an internal review process on CbC-related exchanges, Gibraltar concluded other bilateral agreements consistent with the CbC Bilateral Competent Authority Agreement. These include Guernsey, Isle of Man and the United States and are operational under the relevant articles of their respective TIEAs that allow for automatic exchange of information.

Whilst not among the four BEPS Minimum Standards, Gibraltar adopted key similarities of Action 12 regarding Mandatory Disclosure Rules for aggressive tax planning schemes via the transposition of an equivalent EU Directive. This directive implemented the key elements for a mandatory disclosure regime: (1) a description of arrangements subject to disclosure, (2) a description of the persons required to disclose the arrangements, (3) the trigger for the obligation to disclose, (4) a description of the reportable information and (5) appropriate sanctions to address non-compliance. Gibraltar's regime focuses on arrangements that have the effect of undermining reporting requirements under agreements for the automatic exchange of information (CRS/FATCA) or which take advantage of the absence of such exchanges and arrangements that obscure beneficial ownership and involve the use of offshore entities and structures with no real substance. Reporting obligations are objective and not subject to the main benefit test; disclosures are reportable even if the arrangement does not generate a tax advantage.

The use of crypto assets in cross border transactions to store value outside a jurisdiction of residence is increasing. These assets lack visibility and are outside the scope of existing reporting standards and frameworks, such as the CRS. The OECD has developed a new Crypto-Asset Reporting Framework (CARF) to prevent the erosion of advances in global tax transparency and cooperation by the increased use of such assets.

On 10 November 2023, Gibraltar along with several other jurisdictions, issued a joint statement on the implementation of the CARF; an independent initiative welcomed by the OECD Global Forum Secretariat, as part of its ongoing commitment to meet global standards for exchange of information. The widespread, consistent, and prompt implementation of the CARF will further improve the ability to ensure tax compliance and clamp down on tax evasion. The intention is to transpose the model rules into domestic law and activate exchange agreements by 2027.

In 2022, Gibraltar was part of a consensus of 139 jurisdictions that agreed to a joint Statement on the Two-Pillar Solution to Address the Tax Challenges Arising from the Digitalisation of the Economy. Gibraltar continues working on its OECD Pillar Two strategy. Gibraltar announced in December 2023 that its approach to the OECD's Pillar Two Framework will include the implementation of a "Qualifying Domestic Minimum Top-up Tax" applicable as from 2024 and an "Income Inclusion Rule" with effect from 2025.

Between 2019 and 2023, only 16 of the MLA requests received (0.06%) were in connection with tax crimes. Gibraltar can also provide assistance MLA in connection with tax crimes.

11.4 Strategic Approach

The recognition and commitment to implementing principles of good tax governance is inherent in Gibraltar's participation as both a Global Forum member and as an active participant of the BEPS Inclusive Framework.

Whilst BEPS Inclusive Framework members need only implement the four minimum standards, it is an evolving initiative. More actions are likely to become mandatory as measures are developed and introduced to combat tax evasion and profit shifting. Gibraltar fully supports the implementation of the BEPS Action Plans and commits to the adoption of the minimum standards. Promoting good governance, improving international tax cooperation, facilitating the collection of tax revenues and the combatting of illicit flows are pillars applicable to any participating jurisdiction of the OECD's Global Forum and BEPS Inclusive Framework.

The requirements of good tax governance, cooperation and transparency prove that jurisdictions must not only police taxation within their borders but also have an awareness of what occurs elsewhere and engage in active tax cooperation and sharing of information to help combat tax evasion and illicit flows.

The Economic and Financial Affairs Council of the European Union together with the Code of Conduct Group on Business Taxation publishes a list of non-cooperative jurisdictions bi-annually. Third country jurisdictions that are classified as non-cooperative are screened on several criteria including tax transparency, fair taxation, and anti-BEPS measures. Gibraltar's exclusion from the EU's list is due to its significant work in the areas of cooperation and transparency as well as its international membership in bodies at the forefront of implementing global standards.

The Income Tax Office in Gibraltar maintains a positive and constructive relationship with tax administrations, finance ministries and exchange of information authorities of the many jurisdictions it works with and supports good working relationships with international tax organisations, such as the OECD.

The Income Tax Office in Gibraltar also maintains contact with HM Revenue & Customs' Fiscal Crime Liaison Office (FCLO) responsible for Spain, Gibraltar and Andorra. This allows Gibraltar to understand the risks and typologies identified and investigated by the UK enabling Gibraltar to consider key indicators in its domestic risk processes and engage in supporting the pursuit of tax evasion and illicit flows. Most recently, UK's FCLO has identified a typology for payroll fraud using foreign registered umbrella companies. Intelligence sharing, including characteristics of typical corporate structures used by such groups, enables Gibraltar to use its domestic review procedures to support international efforts.

The Income Tax Office also forms part of the Quad Island Forum, an initiative in which the Financial Intelligence Units and tax authorities of the Channel Islands, Isle of Man and Gibraltar meet at least annually to share knowledge, experience, and work collaboratively to combat serious tax-related crimes and sophisticated tax fraud schemes that yield substantial illicit gains. It is a strategic partnership through which criminal activity can be identified and tackled effectively.

Gibraltar's participation in various initiatives on international transparency and cooperation mitigates its exposure to the proceeds of tax evasion.

Statistical information on the exchange of information:

Exchange instrument	2017	2018	2019	2020	2021	2022	2023
Council Directive 2011/16/EU	23	33	20	15	-	-	-
OECD Multilateral Convention	3	16	14	7	10	19	8
Tax Information Exchange Agreements	29	36	-	-	1	4	3
Other bilateral tax agreements	-	-	-	7	19	13	30
Totals	55	85	34	29	30	36	41

TABLE 37 - STATISTICAL INFORMATION ON THE EXCHANGE OF INFORMATION

The Income Tax Office has received 310 requests during the calendar years 2017 to 2023 inclusive. Over 95% of the requests received in these periods relates to suspected under-declaration of tax using either a bank account held in a Gibraltar financial institution to conceal offshore assets or wealth or a structure including a Gibraltar-registered entity obscuring beneficial ownership outside scope of the requesting jurisdiction.

The overall figures show a decline in the number of requests during the latter half of this period. Gibraltar believes this is attributable to the global pandemic and the inability of partner jurisdictions having been able to progress their tax investigations. Gibraltar has also noted a shift towards more detailed and complex requests that invariably take longer to prepare and compile.

In cases where Gibraltar receives a valid request for beneficial ownership information, the Gibraltar authorities are able to obtain the information from the Registrar of Ultimate Beneficial Ownership as a relevant authority designated for such purposes, supporting the view that the domestic framework ensures that information concerning beneficial ownership is adequate, accurate and timely. If beneficial ownership information is unavailable from the Registrar, due to a request focusing on periods outside the scope of the commencement of the ultimate beneficial ownership register in Gibraltar, the tax authorities issue a statutory notice as part of their administrative enquiries to seek the information directly from the party concerned or their designated trust and company service provider. A greater dialogue with the Gibraltar Financial Services Commission as the supervisory authority addresses any potential failure by regulated entities in their capacity as trust and company service providers. The Gibraltar tax authorities obtain accounting and banking information validly requested by treaty partners via the administrative enquiry process through the issue of a statutory notice. There have been no instances within the period extending from 2017 to 2023 where the Gibraltar tax authorities have declined a valid information request by a treaty partner.

Following the introduction of the newer tax transparency standard regarding automatic exchange of information and the requirement for an administrative compliance framework, the Gibraltar tax authorities are required to ensure financial institutions in Gibraltar are complying with the requirements of the CRS. A major part of the CRS is the requirement for financial institutions to identify account holders (including the controlling persons) for accounts held by entities in accordance with defined due diligence requirements.

The Income Tax Office in Gibraltar continues to consider a proposal for the implementation of an external audit requirement under which financial institutions in Gibraltar are required to obtain an externally certified auditor's report confirming adherence to the due diligence

requirements stipulated under the transparency standard. The relevant gateway with the Gibraltar Financial Services Commission will allow closer dialogue and cooperation with such supervisory authorities in sharing concerns to plan enforcement actions or the imposition of sanctions.

Through its various international agreements, Gibraltar may potentially receive requests for tax information from over 130 jurisdictions; this includes the OECD Convention on Mutual Administrative Assistance in Tax Matters, which is the most widely used tool now used for the exchange of tax information. Gibraltar relies on tax transparency to prevent and detect potential abuses of its financial system for tax crimes underlying money laundering, such as tax evasion. Gibraltar is strongly committed to tax transparency. It has taken considerable steps to promote and ensure it can effectively exchange tax information on request, automatically or spontaneously.

The actual requests received by Gibraltar across the period analysed from 2017 to 2023 remains relatively low meaning that the risk of the use of Gibraltar to launder funds derived from tax evasion (such as income tax fraud and other types of tax fraud committed abroad) is low.

Regarding automatic exchanges under the CRS, in 2022 (related to 2021 data) and 2023 (related to 2022 data), Gibraltar sent information on a total of 46,754 and 46,732 financial accounts to other jurisdictions. Despite its active participation in the CRS MCAA, in which more than 140 partner jurisdictions participate that could potentially transmit a request following up the automatic exchange of financial account information, the number of requests received by Gibraltar remains low. It is important to consider that the countries in scope of these exchanges represent a significant population of billions of individuals.

11.5 Conclusion

The numbers of requests that Gibraltar received do not point to it being a significant target jurisdiction involved in international tax evasion. Consequently, Gibraltar does not consider that tax crimes pose a significant risk.

12 Summary of risks, threat and vulnerability scores

By way of summary the following tables summarises the threat, vulnerability and combined scores for ML and FT of each of the risks identified in this NRA. The table by itself is not a substitute to a full understanding of the risks and their mitigation as described in full detail above.

Ref	Risk Description	Money Laundering Risks			Terrorist Financing Risks		
		Threat	Vuln.	Score	Threat	Vuln.	Score
4.1	Spain	4	3	7	4	3	7
4.2	Morocco	4	3	7	4	3	7
4.3	United Kingdom	3	1	4	2	1	3



4.5	High Risk Jurisdictions	3	2	5	2	1	3
4.5.1	FATF High Risk Jurisdictions	3	2	5	2	1	3
4.5.2	Conflict Zones	2	2	4	4	1	5
4.5.3	Drug Trafficking/Producing Countries	2	2	4	2	1	3
4.6	EU and EEA Jurisdictions	2	2	4	3	2	5
		Money Laundering Risks			Terrorist Financing Risks		
	Transnational Crimes	Threat	Vuln.	Score	Threat	Vuln.	Score
5.1	Organized Crime Groups	3	3	6	1	2	3
5.2	Tobacco	3	3	6	1	2	3
5.3	Drug Trafficking	3	3	6	1	2	3
5.4	Fraud	3	3	6	1	1	2
5.5	Cyber Enabled Fraud	3	3	6	1	1	2
5.5	Money Laundering	3	3	6			
5.7	Bribery and Corruption	2	1	3	1	1	2
5.8	Cash & Cash Couriers	2	2	4	1	1	2
5.9	Trade Based Money Laundering	1	1	2			
5.1	Modern Slavery, Human Trafficking & Migrant Smuggling	1	1	2	1	1	2
5.11	Illegal Wildlife Trade	1	1	2	1	1	2
		Money Laundering Risks			Terrorist Financing Risks		
	Banking Sector	Threat	Vuln.	Score	Threat	Vuln.	Score
6.1.1	Deposit Taking	4	2	6	2	2	4
	Corporate Banking	3	2	5	2	1	3
6.1.2	Broker Deposits	2	1	3	1	1	2
6.1.3	Lending Activities	3	2	5	1	1	2
	Safe Custody	1	1	2	1	1	2
6.1.4	Private Banking/Wealth Management	2	2	4	1	1	2
		Money Laundering Risks			Terrorist Financing Risks		
	TCSP Sector	Threat	Vuln.	Score	Threat	Vuln.	Score
6.2.1	Creation of Legal Entities and Legal Arrangements	4	2	6	2	1	3
6.2.2	Business Activities of Legal Entities and Legal Arrangements	3	2	5	2	1	3
6.2.3	Termination of Legal Entities and Legal Arrangements	1	1	2	1	1	2
6.2.4	Private Companies	3	3	6	2	1	3
	Private Trust Companies	2	1	3	1	1	2



	Private Company limited by guarantee with or without share capital	2	3	5	2	1	3
	Foreign Company carrying on business in Gibraltar	1	2	3	1	1	2
	Public Company	1	1	2	1	1	2
	Limited Liability Partnership	1	1	2	1	1	2
	European Economic Interest Grouping	1	1	2	1	1	2
6.2.6	Trusts	2	1	3	1	1	2
6.2.7	Foundations	2	1	3	1	1	2
6.2.9	Asset Holding & Asset Protection Vehicles	3	2	5	1	1	2
		Money Laundering Risks			Terrorist Financing Risks		
	MSBs and MVTs	Threat	Vuln.	Score	Threat	Vuln.	Score
6.3.1	Currency Exchange	3	2	5	2	1	3
6.3.2	Transfer of Funds	3	2	5	3	2	5
6.3.3	Payment Services	3	1	4	2	1	3
		Money Laundering Risks			Terrorist Financing Risks		
	Securities Sector	Threat	Vuln.	Score	Threat	Vuln.	Score
6.4.1	Broker-Dealers	3	2	5	2	1	3
6.4.2	Multilateral Trading Facilities (MTFs) & Organized Trading Facilities (OTFs)	3	1	4	1	1	2
6.4.3	Portfolio Managers & Investment Advisors	3	2	5	1	1	2
		Money Laundering Risks			Terrorist Financing Risks		
	Funds Sector	Threat	Vuln.	Score	Threat	Vuln.	Score
6.5.1	Private Funds	3	3	6	2	1	3
6.5.2	Alternative Investment Fund Managers	2	1	3	1	1	2
6.5.3	CIS Administrators	2	2	4	2	1	3
6.5.4	Experienced Investor Funds	2	2	4	2	1	3
		Money Laundering Risks			Terrorist Financing Risks		
	E-Money Sector	Threat	Vuln.	Score	Threat	Vuln.	Score
6.6.1	Open Loop	3	3	6	4	3	7
6.6.2	Closed Loop	1	1	2	1	1	2
		Money Laundering Risks			Terrorist Financing Risks		
	DLT & VASPs	Threat	Vuln.	Score	Threat	Vuln.	Score
6.7.1	Custodial Exchanges	3	3	6	2	2	4
6.7.2	Non-Custodial Exchanges and Arrangers	3	3	6	2	2	4
6.7.3	Wallet Providers	3	3	6	2	2	4



6.7.4	Mining	1	1	2	2	1	3
6.7.5	Virtual Asset Teller Machines	1	1	2	1	1	2
6.7.6	Initial Coin Offerings	2	3	5	1	1	2
6.7.7	Peer-to-peer lending	2	1	3	3	1	4
6.7.8	Anonymity-Enhancing Assets & Services	4	1	5	4	1	5
6.7.9	Decentralized Finance	3	1	4	4	1	5
		Money Laundering Risks			Terrorist Financing Risks		
	Gambling Sector	Threat	Vuln.	Score	Threat	Vuln.	Score
6.8.2	Remote Gambling (Betting, Casino, Bingo, Poker)	3	2	5	2	1	3
6.8.3	Land-based Casinos	2	2	4	1	1	2
6.8.4	Betting (land-based)	1	2	3	1	1	2
6.8.5	Bingo (land based)	1	1	2	1	1	2
6.8.6	Lotteries (Gibraltar Government Lottery)	1	1	2	1	1	2
6.8.7	Poker (Offline)	1	1	2	1	1	2
6.8.8	Gaming Machines (non-casino)	1	1	2	1	1	2
		Money Laundering Risks			Terrorist Financing Risks		
	Insurance Sector	Threat	Vuln.	Score	Threat	Vuln.	Score
6.9.1	General Insurance	1	1	2	1	1	2
6.9.2	Long term business	1	1	2	1	1	2
		Money Laundering Risks			Terrorist Financing Risks		
	Other DNFBPs	Threat	Vuln.	Score	Threat	Vuln.	Score
6.1	Real Estate Agents	2	1	3	1	1	2
6.11	High Value Dealers	2	1	3	1	1	2
6.12	Legal Profession & Notaries	3	2	5	1	1	2
6.13	Auditors and Insolvency Practitioners	2	1	3	1	1	2
6.14	Accountants	3	2	5	1	1	2
6.12	Tax Advisors	3	1	4	1	1	2
6.13	Pension Advisors and Scheme Operators	2	1	3	1	1	2
6.14	Domestic Football League	2	2	4	1	1	2

End of 2025 National Risk Assessment