TERRORIST FINANCING RISK ASSESSMENT 2025

VIRGIN ISLANDS TERRORIST FINANCING RISK ASSESSMENT 2025

Executive Summary

The Virgin Islands (VI) first assessed its TF risk in 2020, at which time it considered its exposure to TF at both a national and sectoral level. The findings of this initial TF Risk Assessment concluded that the TF risk to the VI was low in relation to domestic TF activity and medium low in relation to TF from international exposure.

Since that time the VI has sought to enhance its understanding of its TF risk exposure and has chosen to update its TF Risk Assessment to reflect current threats and vulnerabilities identified that allow for the propagation of such risk. In order to so, a Working Group was formed comprising all relevant agencies from LEAs, the prosecution, the FIU, the supervisors, the competent authority for International Requests and the sanctions' unit who provided their expertise and experience as well as the data from their agencies in order for a detailed analysis to be conducted[1]. Additionally, information from counterparts and global typologies and open-source material was also considered.

A determination was made as to which countries posed the highest risk for terrorism and terrorist financing (Tier 1 and Tier 2 countries) and all possible links with these countries were examined for each regulated sector as well as for areas such as LPLAs, the use of cash and Non-Profit Organisations (NPOs).

The risk of the use, collection and movement of funds for the purposes of TF in the VI was assessed. The risk of the use of terrorist funds and the collection of terrorist funds was found to be Low. The risk of the movement of terrorist funds through the VI (directly or indirectly) was found to be Medium-High.

In order to assess the risk of movement in a more detailed manner, four typologies were identified by the WG and were assessed as to the risk that they could be misused for the purposes of TF.

[1] A detailed breakdown of data reviewed is contained in the 'data source' list.

The highest risk typology by which the movement of terrorist funds could occur in the VI was VI legal entities being abused for TF purposes (typology 1), this was found to be of Medium-High risk. This was followed by the use of the VI entities as a conduit for the transit of funds that are intended to be used for terrorism purposes abroad, with funds being sent via a VI entity (typology 2), the highest risk entities by which this may occur are VASPs (MH), whereas the risk of misuse via banks and MSBs was found to be lower (L and ML), however, given the risk posed by VASPs this was given greater weighting, providing an overall risk rating of MH for this typology.

The remaining two typologies were found to be lower risk. The risk of VI service providers (Financial Institutions (FIs) and Designated Non-Financial Businesses and Professions (DNFBPs)), knowingly or unknowingly facilitating the movement of funds for terrorism purposes, but without the funds actually entering or moving through the jurisdiction (typology 3), was assessed as Medium-Low. The risk of the VI facilitating the movement through or from the VI of cash or precious metals and stones (PMS), or dual use goods as relevant to TF, was found to be Low.

Threats, vulnerabilities and controls were considered as well as materiality. The sectors or areas most vulnerable to TF were found to be Legal Persons, Trust and Corporate Service Providers (TCSPs) and VASPs.

Finally, recommendations were made to mitigate the risks posed including training and outreach on this risk assessment to the public and private sectors respectively, the continued enhancement of additional resources for the RVIPF, training on the misuse of legal persons and ensuring that law enforcement has access to adequate and accurate beneficial ownership information as well as resources in relation to matters concerning the tracing and recovery of virtual assets.

1. Introduction

The VI is committed to playing its role in the global fight against TF. Terrorists regularly adapt how and where they raise and move funds and other assets to circumvent safeguards that jurisdictions have put in place to detect and disrupt this activity. Identifying, assessing and understanding TF risk is an essential part of dismantling and disrupting terrorist networks[2].

The VI undertook its last Terrorist Financing Risk Assessment (TFRA) in 2020. In 2023, the National AML/CFT Coordinating Council (NAMLCC) issued a statement re-affirming its commitment to strengthening the Territory's Anti-Money Laundering (AML)/Countering the Financing of Terrorism (CFT)/Countering Proliferation Financing (CPF) regime, in which it committed to updating the VI's National AML/CFT Policy, strategy and current RAs at least every two years, to take into account all relevant changes to the threats and vulnerabilities that impact the Territory's risk of Money Laundering (ML), TF and Proliferation Financing (PF) and to ensure ongoing compliance with international standards. It was therefore determined that the TFRA of 2020 was to be updated.

This Risk Assessment enhances the previous findings, considers the latest data and incorporates the findings of separate RAs conducted in 2024, in relation to LPLAs in so far as it relates to TF risk, as well as the TFRA of NPOs. It also takes into account the findings and recommended actions identified in the Territory's 2024 Mutual Evaluation Report (MER), as well as the remediation undertaken since that time. The WG took into account all relevant available data in the consideration of the TF risk, the mitigation of that risk and the next steps to be taken.

As an International Financial Centre (IFC), the understanding of TF risk in the VI is fundamental, given the global nature and complexity of the products and services offered that could increase the jurisdiction's exposure to potential TF. This includes where cross border and complex structures and activities affect the ability of the Financial Investigation Agency - Analysis and Investigation Unit (FIA-AIU) and other LEAs to identify TF cases. It is also

[2] FATF TFRA Guidance, paragraph 1.

important to ensure that FIs[3] and DNFBPs[4] have a robust understanding of risk to assist with the number and quality of Suspicious Activity Reports (SARs) filed in relation to TF.

The main objective of the RA was to assess the jurisdiction's risk exposure to TF in order to (1) deepen the understanding of TF risk by LEAs, other public sector agencies and the private sector (2) deepen the understanding of the TF risks posed by the FI and DNFBP sectors, (3) deepen the understanding of the TF risks posed by the misuse of LPLAs and NPOs, and the use of cash in the jurisdiction and (4) implement/enhance appropriate mitigating measures.

1.1 The Working Group

The WG was composed of members from the following agencies: RVIPF[5] (Financial Crime Unit (FCU) and Intelligence Unit (IU)), Attorney General's Chambers (AGC) (International Cooperation Team (ICT) and National Coordination Team), Financial Investigation Agency – Analysis and Investigation Unit (FIA-AIU), The FIA-Supervision and Enforcement Unit (FIA SEU), Financial Services Commission (FSC), Office of the Director of Public Prosecutions (ODPP), Department of Immigration (DOI), His Majesty's Customs (HMC), Sanctions Coordinator, and the Governor's Office (GO). The WG was established to ensure a wide range of experience and expertise from agencies involved in the Territory's CFT measures. Members were tasked with collecting and analysing data, reviewing findings and considering the appropriateness of applied risk ratings.

1.2 The Regulated Sectors

The following sectors were reviewed under the umbrella of FIs: Banking, MSBs, Insurance, Investment Business (IB), Financing, Insolvency Services[6], VASPs and Virtual Assets (VAs), TCSPs (these were also assessed separately by the LPLAs WG).

The following sectors were reviewed under the umbrella of DNFBPs: Accountants, Lawyers and Notaries, Real Estate Agents, Dealers in Precious Metals and Stones (DPMS) and High-Value Goods Dealers (HVGDs).

[3] FIs include financial institutions, as defined by FATF and as supervised in the VI.
[4] DNFBPs include Designated Non-Financial Business and Professions, as defined by FATF and as supervised in the VI.
[5] The sole LEA responsible for the investigation of terrorist and TF related activities, development and implementation of the Territory's Counter-Terrorism strategy.
[6] Whilst this is not a FI for FATF purposes it is regulated as such in the VI.

1.3 The Tier 1 and Tier 2 Countries

The WG reviewed relevant credible sources such as the Global Terrorism Index (GTI) 2024, issued by the Institute for Economics and Peace, the Financial Action Task Force (FATF) list of countries under increased monitoring[7], the FATF list of High-Risk Jurisdictions subject to a Call for Action, the Corruption Perception Index as well as recent advisories[8] and also considered whether there were any other countries vulnerable to TF with links to the VI. Consequently, two Tiers of countries were identified. Tier 1 countries represent those countries that have a high risk of terrorism or TF activities based on their appearance on the noted lists or indexes. Tier 2 countries represent those countries that have identified TF risk, but the risk is considered less than that of the Tier 1 countries. These two Tiers were used in the assessment of links to countries of higher risk for TF.

The list of Tier 1 and Tier 2 countries as determined by the Terrorist Financing Risk Assessment Working Group was also used by the Legal Persons and Legal Arrangements Risk Assessment Working Group when assessing TF risk to ensure consistency.

TIER 1 – 12 Countries

Burkina Faso, Mali, Pakistan, Syria, Afghanistan, Somalia, Nigeria, Myanmar, Niger, Yemen, Iran, Lebanon.

TIER 2 - 19 Countries

Iraq, Cameroon, Democratic Republic of the Congo, India, Mozambique, Colombia, Chile, Kenya, Philippines, Egypt, Chad, Turkey, Haiti, Algeria, UAE, Saudia Arabia, Qatar, Palestine, Israel.

1.4 The Review Period

The period under review was 2020 to 2023. This was to ensure that there was continuity from the previous RA which considered data between 2015 and 2019, and to enable the most recent available data to be taken into account (namely year end 2023). As the risk assessment

[7] Consideration was also given to countries on the grey list which were not on the GTI in terms of their IO9, IO10, R5 and R6 ratings.
[8] E.g. FinCEN advisory of May 2024

progressed additional information from 2024 became available which was also included to ensure that the risk assessment provided the most up-to-date information available.

1.5 The Methodology

Data was collected and analysed from VI agencies (both members of the WG and outside), regulated entities and from other credible sources[9]. The data was analysed and threats relating to the movement, collection and use of funds were identified and rated. Based on the ratings the threat related to movement was focused on and four typologies identified were assessed, this included the analysis of financial flows involving jurisdictions at higher risk for terrorism or TF. The risk of the movement of cash and PMS for the purposes of TF was also considered. Next, vulnerabilities were considered, first in relation to each regulated sector and in relation to the risk of the misuse of LPLAs for TF, the risk of the misuse of NPOs for TF and the risk of the misuse of cash as well as at the national level. The materiality of the sectors and areas was also taken into account. Finally, the controls were analysed and applied to determine the residual TF risk.

2. Threat Analysis

The FATF defines a TF threat as a person or group of people with the potential to cause harm by raising, moving, storing or using funds and other assets (whether from legitimate or illegitimate sources) for terrorist purposes. TF threats may include domestic or international terrorist organisations and their facilitators, their funds, as well as past, present and future TF activities, and individuals and populations sympathetic to terrorist organisations.[10]

In order to analyse whether identified TF threats related to the collection, movement, or use of funds, data was collected from all relevant agencies including law enforcement as well as international counterparts and the use of open-source information. Additionally, as outlined above, four typologies were identified in relation to the movement of funds and each of these was also assessed. The ratings used to assess the identified threats were Low (L), Medium-Low (ML), Medium-High (MH) or High (H).

The four identified typologies utilised in this RA are:

[9] See data source sheet attached to methodology for full list.
[10] FATF TFRA Guidance, Paragraph 15

- Typology 1: abuse of VI legal entities for TF purposes.
- Typology 2: Use of the VI legal entities as a conduit for the transit of funds that are intended to be used for terrorism purposes abroad, with funds being sent via a VI entity such as a bank, MSB or VASP.
- Typology 3: Facilitation of the movement of funds for TF purposes by VI service providers (FIs or DNFBPs), whether knowingly or unknowingly, but without the funds entering or moving through the jurisdiction or VI entity – for example, VI lawyers providing services to clients that support foreign terrorism.
- Typology 4: Facilitation of the movement through or from the VI of cash, Bearer Negotiated instruments (BNIs), PMS, or dual use goods as relevant to TF).

Data was collected and analysed as it relates to SARs, investigations, prosecutions, potential sanctions breaches and incoming requests for MLA. The RVIPF IU confirmed that there was no other intelligence or information relating to terrorism or TF or related assets in its possession, therefore no terrorism or TF related occurred during the review period. Consequently, there were no terrorism or TF prosecutions or prosecutions and there were no prosecutions relating to any of the Tier 1 or Tier 2 countries during the review period.

2.1 Terrorism

The FIA-AIU received 2 ordinary SARs flagged for potential terrorism in 2020, but it was established these in fact had no link to terrorism. In 2021 one SAR was identified as a 'terrorism-related SAR' but on further analysis was reclassified as a TF SAR and is dealt with below[11]. No ordinary SARs were received in 2022 or 2023 related to terrorism. Between 2020 and 2023, three SARs involving VAs were identified as relating to terrorism,[12] however, they were not assigned for analysis as two of the accounts held at virtual asset exchanges related to these VA SARs were closed and one account seemed to have been abandoned[13]. Each of these matters related to BVIBCs providing VASP services.

[11] The matter was disseminated to a foreign FIU and closed.
[12] In relation to reports regarding VA SARS these were previously categorised as spontaneous disclosures, therefore for the purpose of this review only such SARs from 2022 onwards were reviewed.
[13] It should be noted that subsequently the Standard Operating Procedures (SOP) was updated to outline the need for interim disclosures of such SARs within 5 days with followed up in-depth analysis.

Only one outgoing request was sent by the FIA-AIU in relation to potential terrorism links in the management of a BVIBC, which was sent in 2020, however, no response was received from the requested authority. Further analysis by the FIA-AIU did not reveal any link to terrorism in that matter.

Between 2020 and 2023 the AGC received one incoming Mutual Legal Assistance (MLA) request relating to terrorism, connected to a terrorist organisation. This request related to information sought from a VI company's Registered Agent regarding the activities of a messenger service company registered in the VI.[14] There were no incoming or outgoing extradition requests in relation to terrorism.

Demographics of the Local Population and Movement of Persons[15]

Between 2021 and 2023, of the total 476886 'tourist' classifications, 3,041 'tourists' whose nationalities were of a Tier 2 countries (most commonly Haiti), and 90 'tourists' with nationalities of Tier 1 countries (most commonly Nigeria), entered the VI.

Between 2021 and 2023, 2,738 nationals from Tier 2 countries were recorded as residing in the VI, the majority being from the Philippines. In relation to Tier 1 countries, 178 residents were identified. The most common country of citizenship for residents from Tier 1 countries was Nigeria (60%). There have been no reports, intelligence or other information to suggest any link to terrorism by these groups of persons.

Labour Force Statistics 2020-2023

The number of persons within the VI labour force originating from Tier 1 and Tier 2 countries for the years 2020-2023 is outlined in the table below.

Year	Tier 1	Tier 2
2020	67	1,020
2021	73	1,001
2022	72	1,060
2023	77	1,230

[14] The information was not maintained in the VI as the principal place of business was another jurisdiction. However, the Registered Agent provided the contact information and the location of the business records, which were passed on to the Requesting State.
15 Note this does not include business owners.

The most common Tier 1 countries identified as part of the VI's labour force were Nigeria and Lebanon, while the Philippines was identified as the most common Tier 2 country.

In relation to new work permit holders and newly residing persons, between 2020 and 2023, 814 persons were registered from Tier 2 countries which consisted of new work permit holders, returning work permit holders, new residing persons and government employees for this period. In relation to Tier 1 countries, there were a total of 40 permits of all types as well as residencies registered by DOI.

There has not been any incoming or outgoing information exchange between DOI and counterparts in high-risk jurisdictions, nor any other jurisdiction relating to TF or terrorism. To date, the DOI has not received and does not have any intelligence from any of the high-risk jurisdictions regarding any potential linkages to terrorism, TF nor terrorist organisations relating to residents, work permit holders or visitors.

DOI has seen an annual increase in the number of persons detained in the VI from Haiti and Cameroon directly related to migrant smuggling[16]. These cases, however, are not related to terrorism or TF. The DOI has identified and intercepted several nationals from two Tier 2 countries[17], who intended to migrate illegally to the United States (US) once gaining entry to the VI legally. Within the migrants smuggled, there have not been any linkages to terrorism or TF.[18]

[16] For example, in October 2021, DOI facilitated interviews with Haitian migrants in custody with investigators from country A regarding a migrant smuggling case that was initiated in country A as the confirmed port of embarkation. However, the country A authorities were unable to obtain sufficient documentation for extradition prior to the illegal migrants' repatriation to their home country. The case was not found to be related to terrorism or terrorist financing.

[17] Intelligence from regional agencies suggests that these nationalities traverse various countries seeking means to smuggle to the US

[18] DOI remains cognizant of the risks posed where there are no forms of identification and the potential use of criminal organisations as well as the risk of exploitation of the refugee and asylum processes, although VI does not have law provisions to grant the Haitians and Cameroonians, in attempt to get to the US, apply for asylum upon illegal entry.

Furthermore, HMC noted the risk of vessels entering the Territory, potentially without the requisite documentation for all persons. A 2022 example indicated that HMC discovered a vessel that had arrived without proper clearance and with persons who were subject to Red Notices, they were later detained.[19] Thus far, no such matters have been TF or terrorism related.

The RVIPF and the FIA-AIU have not received any intelligence in relation to Foreign Terrorist Fighters, home grown terrorists (residents or work permit holders) or any incidents of terrorism in the VI.

This analysis supports the conclusion that the threat of terrorism and the threat of the collection or use of funds for the purposes of terrorism in the VI is low, however the emerging threat of migrant smuggling remains under observation, including any potential links to terrorism or TF, which has thus far not been the case.

2.2 Terrorist Financing

Between 2020 and 2023, 100 TF related SARs were received, 88 of which related to VAs. Of the remaining 12, one ordinary SAR (received in 2023) resulted in disclosure to the FCU in 2024. A total of 12 of the 88 VA SARS were disseminated to foreign jurisdictions. 11 of those 12 SARs were also disseminated to the FCU.[20.]

Additionally, the FIA-AIU's outgoing international requests relating to TF increased to 29 in 2023, from 3 in 2022, and 0 in 2021 and 2020.

Furthermore, 2 international requests were received by the FIA-AIU regarding TF. One of these requests related to British Virgin Islands Business Company (BVIBC), which was the subject of the request and one related to a BVIBC operating as a VASP and the misuse of cryptocurrency. One request related to the misuse of a VASP to transact in cryptocurrency with an address labelled "The Forgotten Ones-Pro-Isis Telegram".[21] Another request related to

[19] https://www.thedailyherald.sx/islands/charter-boat-crew-returns-home-after-bvi-detention.

[20]This related to a SAR filed regarding an alleged association between a BVIBC and a terrorist group. Information was received from various relevant jurisdictions. The relevant intelligence was disseminated to relevant foreign jurisdictions and relevant domestic Authorities.

[21] (2022)

potential funding to a Tier 1 country via a bank account held by a BVIBC in a foreign jurisdiction.[22]

During this period, 705 SARs related to identified high-risk jurisdictions were received. A total of 660 of which were crypto related. Thirteen disseminations were made to relevant jurisdictions and the FCU relating to high-risk jurisdictions, 4 of which related to TF (and 6 of which 13 were crypto related). The disseminations were made to the relevant jurisdictions and the FCU. In addition, 87 international requests were received regarding high-risk jurisdictions. None of which, other than those two classified as TF above, were found to be TF related.

The total VA SARs received between 2022 and 2023 was 10,161. During the same time period a total of 20 disseminations were made to the relevant jurisdictions and the FCU.[23] Of these, 9 (45%) related to TF.[24] There were also 17 incoming international requests relating to cryptocurrencies in 2022 and 34 in 2023, 2 of which related to TF. Domestic requests related to VAs were 1 in 2020, 1 in 2021, 8 in 2022 and 10 in 2023. This category of SAR significantly exceeds any other category and signals a potentially elevated threat of the misuse of VASPs generally, as well as for the movement of funds for potential TF purposes.

For VA SARs received between 2022 and 2023, 19 related to TF high-risk jurisdictions, 1 related to terrorism. The countries identified were all Tier 2 countries. Suspicion of fraud was the largest category with 105 VA SARs recorded. The general suspicion of ML was the second largest category with 87. For ordinary SARs received between 2020 to 2023, 1 related to TF and 1 related to terrorism. The largest number of SARs related to high-risk jurisdictions was in relation to a Tier 2 country, with a total of 17. The second largest number was 16 relating to another Tier 2 country. Lack of customer due diligence (CDD) was the most common issued identified (25 SARs)[25]. Fraud and ML were each identified in 8 SARs.

[22] (2022)
[23] Prior to 2022 virtual asset reports were considered information disclosures rather than SARs
[24] In addition to TF, other suspicions included Child Sexual Abuse Material, fraud, embezzlement, cybercrime, theft.
[25] It is noted that after 2022, the method of categorising offences changed, and lack of CDD was excluded as an 'offence'.

In 2022, 3 disseminations were received by the FCU from the FIA-AIU in relation to TF and 3 investigations were commenced. In 2023, 8 disseminations were received in relation to TF and 8 investigations were commenced.[26] The RVIPF-FCU provided 14 cases studies[27] in relation to TF investigations commenced. All matters relate to BVIBCs. These are all ongoing investigations.

13 of the investigations relate to BVIBCs operating VASP platforms and the potential misuse of these platforms. The final matter relates to the use of a dissolved BVIBC's bank account to send and receive funds. Therefore, all cases fall into typology 1, with the majority also falling into the more specific typology 2. Both typology 1 and typology 2 were found to be Medium High Risk, for typology 2 this particularly related to the movement of VAs through VASPs.

No disseminations were received by the FCU from the FIA-AIU regarding VAs in 2020 and 2021. In 2022, three TF investigations commenced based on disseminations all of which involved BVIBCs offering virtual asset services. In 2023, 10 disseminations were made to the FCU in relation to VAs. A total of 8 of these disseminations were related to TF and investigations were commenced.[28]

Since 2020[29] the RVIPF FCU has received a total of 14 disseminations relating to funds or virtual assets being moved for the purpose of financing terrorism. The disseminations received do not always identify the terrorist organisation involved, which may be unknown.[30] None of the matters under current investigation relate to the collection or use of funds or virtual assets for the purpose of TF. 13 of the disseminations relate to BVIBCs acting as VASPs which may have facilitated the movement of funds via a platform and all 13 investigations relating to the misuse of VASPs for TF are under investigation by the FCU. One TF investigation opened in 2024 following a dissemination from the FIA-AIU did not involve a VASP but involves a complex multi-jurisdictional investigation into the suspected use of a dissolved BVIBC's bank

[26] As of August 2024, 2 disseminations had been received regarding TF and 2 investigations commenced.
[27] 3 from 2022, 8 from 2023 and 3 from 2024.
[28] As of August 2024, 1 dissemination had been made to the FCU regarding virtual assets, which was not alleged to relate to TF.
[29] There were no disseminations received by the RVIPF from the FIA-AIU or any other source in relation to terrorism or terrorist financing in 2020 or 2021 and no investigations were commenced. In 2022 there were 6 disseminations, 3 of which were TF, in 2023 there were 10 disseminations, 8 of which were TF. (In 2024 3 TF disseminations were received).
[30] Information may be received from the blockchain analytical tool which flags the matter as associated to TF without necessarily providing information as to the exact Terrorist Group in question.

account to transfer money. These investigations are in the stage of evidence collection to establish whether there is sufficient evidence to submit to the ODPP for charge.
Other than the FIU disseminations received by the FCU and described above, there have been no incoming international cooperation, MLA or LEA requests received by the FCU regarding TF, terrorism or high-risk terrorist countries for the period 2020 to 2023.

Between 2020 and 2023, one incoming MLA request was received by AGC relating to purported TF connected to a terrorist organisation. However, the request did not comply with the legal threshold for providing MLA as there was no ongoing criminal investigation in the Requesting State and an insufficient nexus was provided in relation to the two VI companies into which the request was made.

There were no incoming or outgoing extradition requests relating to TF. A total of 24 MLA requests were received from Tier 2 countries (the majority related to service of documents), (none from Tier 1 countries) during the reporting period, however none of these related to terrorism or TF.[31] There were no outgoing requests to any Tier 1 or Tier 2 country.

Between the period 2020-2024, the FIA-Supervision Enforcement Unit (SEU) documented one case where a lawyer provided litigation services to a company with alleged close ties to a terrorist organisation (the lawyer was not conducting relevant activities for the purposes of AML supervision) (Typology 3). This matter was disclosed to the FCU and to foreign FIUs by the FIA-AIU.

RVIPF IU did not receive any requests from international counterparts where TF was the primary offence.[32] A total of 120 Interpol requests were received in 2023, 65 of which were sent to the FIA-AIU. None of those requests were from Tier 1 or 2 countries, however over half were from the Baltic region. No data could be obtained for the years 2020-2022 due to technical issues with the International Criminal Police Organisation (INTERPOL) system. It is unknown by RVIPF Intelligence whether these requests were in relation to sanctions or if they were TF related, as the member country does not state the reason for the request. RVIPF Intelligence does not collect the figures for non-FIA-related requests

[31] 13 related to the service of documents in civil matters, 3 did not show a nexus to the VI and the remaining 8 related to other criminal offences relating to BVIBCs, and the information was provided
[32] Other offences are not noted.

As part of the RA process, the RVIPF reached out to their most frequent counterparts directly and utilising the informal network of Arin Carib, no relevant information was identified concerning any known terrorism or TF threat to the VI.

2.2.1 Targeted Financial Sanctions Breaches Relating to Terrorist Financing

As demonstrated in the table below, there were a total of 39 SARs filed regarding breaches of Targeted Financial Sanctions (TFS) relating to TF:

SARs - TF TFS	2020	2021	2022	2023
Ordinary SARs	1	1	0	1
VA SARs	N/A	N/A	5	31

While TFS disseminations were made to the Governor's Office between 2020 and 2024, in relation to non-TF sanctions' breaches, no disseminations were made to the FCU relating to TF-TFS between 2020 and 2023 (nor to the Governor's Office). However, in 2024, one dissemination was made in relation to TF-TFS sanctions (to the FCU and the GO) and an investigation commenced.

There were no requests for designation during the review period and no licences requested or granted relating to persons designated under the TF sanctions regimes. The Governor's Office was notified by a Competent Authority of the designation of a beneficial owner of 9 BVI Companies on another country's Sanctions List. The said sanctioned individual was said to be potentially linked to a terrorist organisation. The 9 BVI companies associated with this designated person were not sanctioned by any UK or UN Sanctions Regimes. This information was further shared with several other jurisdictions.

Since June 2023, the GO has received an increase in suspected/attempted sanctions breaches involving funds being transited through VI VASPs. During 2023, these related to the Russian sanctions regime. The movement of funds VAs through VASPs (typology 2) is therefore increasing in prevalence.

The data gathered above points to an elevated risk of the misuse of VASPs in the VI for moving funds for the purposes of financing terrorism and/or breaching TF-TFS. The figures demonstrate that the misuse of VI entities in the movement of funds or VAs is the highest risk (and that collection and use of such funds are low risk) and that this particularly relates to the misuse of VASPs and the movement of VAs.

2.2.2 The Misuse of British Virgin Islands' Business Companies for Terrorist Financing

Between 2020 and March 2024, the FIA received 13 TF SARs relating to BVIBCs. All the TF SARs that involved a legal person or arrangement related to a BVIBC (and not another type of legal person or arrangement). The FIA disseminated 13 disclosures relating to TF connected to BVIBCs to the FCU. Moreover, 12 of the 13 SARs disseminated were filed by a BVIBC that was carrying out activities involving VAs. Only one SAR disclosed suspicion of a BVIBC's involvement in TF.

Between 2020 and 2024, the RVIPF opened 14 investigations relating to TF involving legal persons. One of the TF investigations related to a suspected sanctions breach with a TF element. Each investigation related to BVIBCs (3 in 2022, 8 in 2023 and 3 in 2024). There were no investigations into foreign companies, other types of legal persons or trusts.

MLA figures for requests received from third countries between 2020 and 2024, show one incoming request involving a BVIBC relating to terrorism and one relating to TF. There were no other requests relating to any other types of LPLAs in relation to TF.

The threat rating for BVIBCs[33] in the LPLA RA was Medium-High, the threat rating for other LPLAs was Low. As BVIBCs are by far the largest sub-set of all LPLAs, and 99% of these are BVIBCs limited by shares, this is the rating used for this RA.

2.2.3 The Misuse of Cash for Terrorist Financing

Whilst SARs filed in relation to cash deposits have increased (2020 – 15, 2021 – 41, 2022 – 105, 2023 – 28) and SARs are received concerning unknown source of cash deposits, no analysis of such SARs has led to a TF suspicion. Furthermore, according to the RVIPF IU,

[33] BVIBCs are by far the largest sub-set of all legal persons and legal arrangements types in the VI. There are 5 possible types of BVIBCs. BVIBCs limited by shares represent approximately 99% of all BVIBCs (paragraph 26, LPLA RA).

there is no intelligence on record to suggest any TF offences occurring using cash intensive businesses or via the movement of cash.

The FCU has received no information passed through by intelligence, either from the FIA or any other source, relating to cash being moved through the territory relating to TF. The instances of cash misuse emanate primarily from the importation/possession of controlled drugs or failing to declare cash over $10,000 being discovered at the border. There is no evidence that any of these seizures involve Tier 1 or Tier 2 countries.

The movement of cash throughout the VI has primarily been by way of cargo vessels and go-fast vessels and has on occasion been used for drug transactions.[34] There has been no link to TF in any of the interceptions conducted.

In relation to cash intensive businesses such as car hire companies, launderettes, construction companies, local music industry, car washes, hair salons, restaurants/bars, maritime services, there is no intelligence to suggest any TF offences may be occurring.

Informal Transfer Services Such as Hawala or Alternatives

During the relevant period, the RVIPF FCU has not received any direct intelligence to support the existence of informal transfer services such as Hawala or any alternatives, and there was no intelligence, SARs or other information indicating any link between the use of Hawala or any other informal transfer service and the VI. Furthermore, the FSC policing the perimeter has not found any such system.

The frequency and value of the movement of cash or BNIs in and out of the jurisdiction was considered, as well as whether any such movement had any links to terrorism or TF, or generally to higher-risk jurisdictions. Cash seizures by law enforcement were also considered in terms of their frequency and value, as well as any link to terrorism or TF or any high-risk jurisdiction. Intelligence gathered by the RVIPF IU on the misuse of cash (or BNIs), the

[34]in 2020, two persons were arrested following a chase by officers from Customs, Immigration and the police force, with over $800,000.00 on a go- fast vessel, they were later convicted of offences including possession of proceeds of criminal conduct and failing to declare money: Duo found with $805K in BVI waters found guilty! $$ forfeited to Crown (bvinews.com). The carrying of cash just below the $10,000 threshold, primarily to the Dominican Republic, was noted by HMC to have subsided in recent years.

frequency of such reports, the amounts, the level of concern and any links to terrorism, TF or high risk jurisdictions as well as information held by the FIA-AIU (SAR filings, international requests etc.) were considered and it was concluded that whilst the misuse of cash posed a threat, the threat in relation to the misuse of cash for TF purposes was low.

2.2.4 The Movement of Goods and Precious Metals and Stones

During the years 2020-2023, goods (mainly clothing, furniture, stationery, jewellery) were declared upon importation through the Customs Automated Processing System via a Trader Declaration and these declarations were analysed.

Goods in the VI are primarily imported from the US mainland. There has also been an increase of importation of goods from China, but none from high-risk TF countries. There has never been an interception of goods destined for high-risk countries where such goods were being transited through the VI.

In 2021, jewellery originating from a Tier 2 country was imported from the US to the VI seven times, via ferry terminals and carried by the passenger, each contained a stamped declaration form from US Customs[35]. Other goods, originating from a Tier 1 country were imported through the airport. HMC reviewed these matters and confirmed there was no link to TF. In relation to the movement of PMS, the route used appeared to be from Country A to Country B and onwards to Country C. There was no suspected link to TF

Neither the RVIPF FCU nor the FIA-AIU had received any intelligence from any source relating to the movement of PMS for the purposes of TF. As such, the RVIPF FCU has conducted no investigations in relation to the movement of PMS. In relation to the movement or smuggling of goods including cash, BNIs and PMS, the RVIPF IU received no information or intelligence relating to TF. Furthermore, there was no intelligence in relation to significant links to Tier 1 or Tier 2 countries, or to TF or terrorism. No vessels were registered to a legal owner in a Tier 1 or Tier 2 country or had any links to terrorism or TF.

[35] On one occasion it was ascertained that the passenger was enroute to another jurisdiction as there were no direct flights.

Therefore, in relation to the movement of goods and the movement of PMS there has been no suspicion of, or information in relation to, TF.

2.2.5 The Misuse of Virgin Islands' Non-Profit Organisations for Terrorist Financing[36]

Between the period 2021-2023, based on data collected from the RVIPF, there were no intelligence-led investigations, criminal investigations or allegations in credible open sources related to TF involving VI NPOs or their representatives (including employees, volunteers or other individuals acting in an official capacity representing an NPO). The FIA-AIU indicated that during the period 2021-2023, there was no intelligence received in relation to VI NPOs or their representatives being involved in TF and there were no STRs/SARs received related to TF involving NPOs or their representatives (including employees, volunteers or other individuals acting in an official capacity representing an NPO). During the period of 2021 – 2023, there were no NPO related case files (TF or otherwise) submitted to the ODPP and no TF prosecutions or convictions.

The NPO TFRA (2024) found that the level of TF abuse is low for all categories of FATF NPOs. This is evidenced by the data collected from the relevant LEAs, with no reports of TF-related SARs, intelligence investigations, prosecutions, convictions or SARs in relation to any NPOs or their representatives, within the period of 2021-2023. The level of foreign TF threat is Medium-Low on account of a few FATF NPOs with affiliation, control structures and disbursements connected to Tier 1 and Tier 2 jurisdictions during the period of 2021-2023. The domestic terrorist threat is low in the VI based on intelligence from LEA with no records of known terrorist groups, organisations and/or terrorist fighters or self-radicalised terrorists operating in or targeting the VI.

2.3 TF Open Source case studies – Legal Persons and Legal Arrangements

In addition to the information in the possession of the VI agencies, other reliable sources were also researched to gather information about the misuse of the VI for the purposes of terrorism or TF.

[36] In accordance with FATF Recommendation 8, the VI undertook a domestic review of the entire NPO sector to identify the NPOs that fall within the scope of the FATF definition of a NPO, to assess the terrorist financing risks facing FATF NPOs, to identify the subset of NPOs which are most at risk for TF abuse and to determine the adequacy of the laws, regulations, and other measures in place to mitigate those risks, this risk assessment was completed in 2024.

Eight cases were found during an open-source search relating to TF and VI entities. In terms of the type of VI entities utilised, BVIBCs featured most prominently.

In one case, a business within a tier 1 country with alleged ties to a convicted war criminal and supporter of a terrorist group[37] used a VI-registered company[38] as part of a broader financial network to facilitate illicit transactions. These examples highlight how VI companies can be exploited for illicit financial flows linked to terrorism.

In another case, VI companies were seen to be used as fronts to move funds through the US financial system for the benefit of a State Sponsor of Terrorism[39].

Other cases identified potential direct and indirect links to terrorists and terrorist organisations worldwide. In these cases, VI companies were allegedly used as front companies for illicit funds movement, or as part of complex structures allegedly used to fund individuals linked to terrorist organisations.

In another matter, highlighted in the LPLA RA, an individual resident in Country 1, a country known to support terrorism, operated several companies around the world in the real estate, food processing and diamond industries. The individual used the profit from his companies to purchase properties to be used by known terrorist organisations and to engage in trade-based money laundering. The individual incorporated a BVIBC, which shared a name and was a subsidiary of a company in Country 1, as part of the worldwide corporate structure to facilitate the transfer of funds to the terrorist organisation. The individual became designated under a counter-terrorism TFS regime.[40] However, the individual's name did not appear on the ownership records for the VI entity. This example shows how terrorist financiers and

[37] BBC News - Taylor Sierra Leone war crimes trial verdict welcomed https://www.bbc.com/news/world-africa-17864387
[38] Letter dated 12 December 2008 from the Acting Chairman of the Security Council Committee established pursuant to resolution 1521 (2003) concerning Liberia addressed to the President of the Security Council. https://digitallibrary.un.org/record/643642?ln=en&_gl=1*545a1h*_ga*Nzc5MjI4NjI5LjE3MjcyOTg0OTU.*_ga_TK9BQL5X7Z*MTcyNzM2NTk3NS4zLjEuMTcyNzM2NzE0NC4wLjAuMA..&v=pdf#filesv
[39] US District Court Indictment, Washington Post, https://www.washingtonpost.com/world/national-security/us-charges-four-chinese-nationals-and-a-chinese-company-with-aiding-pyongyangs-nuclear-program/2016/09/26/1a7a4b16-8407-11e6-92c2-14b64f3d453f_story.html
[40] LPLA 2024, case study.

designated persons seek to obscure the BO of legal persons and obscure the flow of funds through complex multi-national corporate structures.

The LPLA RA found that local and international typologies research uncovered recent cases involving suspected TF involving BVIBCs and several terrorist organisations. Moreover, four of the five cases related to misuse of a VASP to carry out the TF. The number of cases, and the fact that many different terrorist organisations are named, suggests that BVIBCs are more susceptible to misuse by terrorist financiers. No typologies were found relating to other types of legal persons and none related to legal arrangements.[41]The cases analysed show that VI entities are found in complex, international structures that could be set up for the benefit of sanctioned individuals, terrorist suspects and those linked to terrorist groups or regimes. As such, the threat rating from the typologies review exercise suggests a high threat level for misuse of VI LPLAs by those seeking to evade sanctions related to terrorism or for TF.

2.3.1 Terrorist Financing Case Studies – Virtual Assets

While cash, hawala, and traditional money services remain the default tools for TF, the research of a reputable Blockchain firm found a growing interest in cryptocurrencies by terrorist groups and their supporters. Among cryptocurrency addresses linked to terror financing campaigns, there was a 125% increase in TRON addresses in 2023, compared to a 12% increase in Bitcoin addresses.[42] In particular it was seen that a stablecoin issuer that provides USDT, a fiat-pegged digital asset, across multiple blockchains, including TRON, has VI entities in its structure that are directly involved in the issuance and management of USDT on the TRON blockchain. Specifically, a VI business helps manage how USDT works on different blockchain networks, including TRON. This allows people to send, receive, and use USDT easily within the TRON system, making it compatible with various apps and services on that network.[43]

[41] In relation to legal arrangements, as noted above, there were also no law enforcement cases or SARs or MLA requests relating to LA and TF.
[42] TRM The Illicit Crypto Economy – key trends from 2023. Noting that a BVIBC issued TRON.
[43] Businesswire.com - TRON Collaborates with Tether to Issue USDT Tokens https://www.businesswire.com/news/home/20190304005852/en/TRON-Collaborates-with-Tether-to-Issue-USDT-Tokens?utm_source=chatgpt.com

Four cases involving VAs and TF/TFS were located during an open-source search. All cases involved the alleged misuse of cryptocurrency trading platforms and two related to a trading platform, which was launched by a BVIBC.

In one reported case, offshore entities, including two VI entities, played a role in a Financial Crimes Enforcement Network (FinCEN) regulatory case. One VI-registered entity, affiliated with Customer A, continued trading on the platform in question (Finance) despite US regulatory concerns, while maintaining a material presence in the US through its affiliates. Another VI entity, Customer C, facilitated institutional market participants' access to various cryptocurrency exchanges, while having clear ties to the US. By facilitating access to the platform, through nested exchanges and sub-accounts, these entities enabled high-risk transactions, including those involving illicit actors, without sufficient safeguards. According to the FinCEN Consent Order, user addresses on this platform transacted with wallets linked to designated terrorist organisations. FinCEN observed hundreds of direct transactions with these organisations, amounting to several hundred thousand dollars, and the platform failed to file SARs on these transactions, despite being aware of the risks, with internal communications describing flagged transactions as "extremely dangerous for our company". A project linked to this platform (Finance) recently established a subsidiary in the VI to enhance its strategic Bitcoin asset management[44] and a VI AIM licence was also granted to a project associated with the same trading platform[45]. This may make the VI vulnerable to additional TF risk related to mixing traditional finance with decentralised finance (DeFi). These platforms often allow anonymous transactions, making it easier for criminals to move money without being detected, and tokens may be used to move funds across borders without raising alarms due to differences in regulations. Privacy tools built into DeFi make it harder to track where money comes from, and criminal funds deposited into high-yield products can later be withdrawn as "clean" cash. Since these platforms aren't fully centralised, stopping or reversing suspicious transactions is much more difficult.[46].

[44] Finance Square – Metaplanet Establishes Subsidiary in British Virgin Islands for Strategic BTC Asset Management https://www.Finance.com/en-NG/square/post/2024-06-25-metaplanet-establishes-subsidiary-in-british-virgin-islands-for-strategic-btc-asset-management-9942958839538
[45] Finance Square - BounceBit obtains AIM licence in the British Virgin Islands https://www.Finance.com/en/square/post/02-14-2025-bouncebit-aim-20282376543074
[46] FinCEN

There is evidence that terrorist organisations are accessing virtual asset trading platforms, and that such platforms are making it easier for those organisations to raise money outside of their countries of origin.[47] Middle Eastern terrorist organisations are alleged to have utilised a particular trading platform to raise funds and move significant sums, as are other terrorist groups and sanctioned individuals. VI entities that facilitate access to such platforms, even indirectly, create vulnerabilities that could be exploited for laundering illicit funds, including those linked to TF.

A separate exchange with a VI link was utilised in a large-scale crypto scam, as well as being used by multiple Jihadist organisations engaging in crypto asset-enabled fundraising[48].

The cases analysed show that VI entities are at risk of being involved indirectly in the misuse of VAs for TF or the evasion of TFS. VAs are attractive to terrorists, sanctioned individuals, and other criminals due to the lack of cohesive global regulation, the ease with which the origin of funds may be disguised and the fast pace at which new technology develops. The misuse of one trading platform by an international crime organisation,[49] as well as purportedly by multiple terrorist groups using similar methods[50], further underlines the appeal of this type of platform to those seeking to move illicit funds internationally. The presence of VI entities in complex, global ownership and control structures for virtual asset service providers can enable those providers to blur their ultimate ownership and accountability, and potentially play an indirect part in illicit activity, including terrorist funding, that utilises these networks. These

---

https://www.FinCEN.gov/sites/default/files/enforcement_action/2023-11-21/FinCEN_Consent_Order_2023-04_FINAL508.pdf
US Department of Justice
https://www.justice.gov/opa/pr/Finance-and-ceo-plead-guilty-federal-charges-4b-resolution#:~:text=%E2%80%9COur%20team%20of%20investigators%20uncovered,International%20Emergency%20Economic%20Powers%20Act.
The Guardian
https://www.theguardian.com/technology/2024/apr/30/Finance-founder-sentenced-money-laundering#:~:text=Changpeng%20Zhao%2C%20the%20former%20head,itself%20was%20fined%20%244.3bn.

[47] US Department of Justice
https://www.justice.gov/opa/pr/global-disruption-three-terror-finance-cyber-enabled-campaigns

[48] US Department of Justice
https://www.justice.gov/opa/pr/cyber-scam-organisation-disrupted-through-seizure-nearly-9m-crypto

[49] US Department of Justice
https://www.justice.gov/opa/pr/cyber-scam-organisation-disrupted-through-seizure-nearly-9m-crypto
ICIJ - Offshore Leaks Database
https://offshoreleaks.icij.org/nodes/82024464

[50] US Department of Justice
https://www.justice.gov/opa/pr/global-disruption-three-terror-finance-cyber-enabled-campaigns

cases show that the threat level of VI entities being utilised in the misuse of virtual asset services, whilst still emerging, is evident.

2.4 Conclusion of Threats to the Virgin Islands

The threat of domestic terrorism is low. There has never been a terrorism incident and there is no intelligence or information relating to any such potential incident.

The threat of TF in the VI as it relates to the use of funds and the collection of funds is low whereas the threat as it relates to the movement of funds is Medium-High. The conclusion in relation to the four typologies was that typology 1 was of the highest risk at MH, closely followed by typology 2 at MH, (consisting of banks – L, MSBs, ML and VASPs MH), typology 3 was Medium-Low risk (ML) and typology 4 was of the lowest risk (L).

3. Vulnerabilities

The FATF defines vulnerability as "things that may be exploited by the threat, or that may facilitate its activities". The concept of TF vulnerability comprises those things that can be exploited by the TF threat or that may support or facilitate its activities. Vulnerabilities may include features of a particular sector, a financial product or type of service that make them attractive for TF. Vulnerabilities may also include weaknesses in measures designed specifically for CFT, or more broadly in AML/CFT systems or controls, or contextual features of a jurisdiction that may impact opportunities for terrorist financiers to raise or move funds or other assets (e.g. large informal economy, porous borders etc.). There may be some overlap in the vulnerabilities exploited for both ML and TF.[51]

The absence of known or suspected terrorism and TF cases does not necessarily mean that a jurisdiction has a low TF risk. In particular, the absence of cases does not eliminate the potential for funds or other assets to be raised and used domestically (for a purpose other than terrorist attack) or to be transferred abroad.[52] Due to the high volume and cross-border nature of assets managed and transferred, international finance centers may be vulnerable to misuse through the movement or management of funds or assets linked to terrorist activity.

[51] FATF TF Risk Assessment Guidance, paragraph 15
[52] FATF TF Risk Assessment Guidance, paragraph 34

The assessment of vulnerabilities was therefore divided into (1) Vulnerabilities of FIs and DNFBPs and other specific sectors or areas and (2) Structural vulnerabilities including compliance with FATF standards for technical compliance and effectiveness and other vulnerabilities at the national level.

3.1 Vulnerabilities: Individual Regulated Sectors

Each regulated sector was examined in relation to its vulnerability to TF. This involved examining client base, products and services, movement (banking, MSBs, VASPs and DPMS only) and distribution channels to establish any links to TF or TF identified higher risk countries. Consideration of client base included the nationality and/or residence of clients, or BOs of clients, being Tier 1 or Tier 2 jurisdictions. In relation to distribution channels, considerations such as the number of clients onboarded from Tier 1 or Tier 2 jurisdictions as well as the use of online platforms or third-party Eligible Introducers (EIs) based in these jurisdictions were considered. When assessing other links to Tier 1 or Tier 2 countries, it was assessed whether there was a parent, subsidiary or a director in any of these jurisdictions.

Secondly, broader vulnerabilities were considered in relation to each sector, namely, any indication that the SAR filing level was low in relation to the risk rating of the sector, overall implementation of CDD obligations/internal controls across the sector, the level of AML/CFT compliance and awareness within the sector and the scope of unregulated actors for each of the sectors.[53] Finally, the ability of government, law enforcement and/or regulators to share information with the private sector[54] was also considered.

Data was collected and analysed and the expert opinions of those closest to the sectors were sought. The weight of particular factors in relation to their relevance to the sector was also considered in determining the overall vulnerability of each sector.

Financial Flows Between the Virgin Islands and Higher-Risk Jurisdictions

[53] Both as per enforcement and as per information / intelligence (broadly speaking), additionally any gaps in regulatory coverage were considered.
[54] Regular meetings with private sector and whether information is shared, whether information on TF risks / vulnerabilities is shared, how specific / sensitive this can be, whether there is any prohibition on sharing sensitive information, which may lead to further input from private sector (e.g. SAR filing).

Regarding banks, there are no identified fund flows to and from any Tier 1 or Tier 2 jurisdictions for the relevant period. In relation to MSBs, financial flows to and from Tier 1 countries account for less than 1% of all financial flows within that sector[55], while flows to and from Tier 2 countries account for approximately 5%.[56] The countries identified, however, align with the migrant population within the VI.

However, in relation to the VASP sector, given the nascent nature of the regime, currently there is imprecise data to properly identify fund flows to and from Tier 1 and Tier 2 jurisdictions. The geographic location of clientele of VASP applicants is diverse, but with a significant concentration in Europe and Asia. The client base in one of the Tier 2 countries though smaller in size is growing but is still relatively limited. Australia and South America exhibit comparatively lower representation in the clientele demographics. The VASP sector therefore poses a risk in relation to the movement of VAs to and from high-risk TF jurisdictions.

3.1.1 Banking

Banks in the VI are licenced under the Banks and Trust Companies Act, 2020 (as amended) (BTCA). There are currently six commercial banks and one private wealth management institution that make up the banking sector within the VI.[57] One of the commercial banks is domestically owned with the majority shareholder being the Government of the VI. The other five commercial banks are subsidiaries or branches of international banking groups and apply AML/CFT measures commensurate with their group. These institutions are established in jurisdictions that have been assessed as having equivalent AML/CFT regimes to the VI. While the banking sector is small in terms of the number of licenced institutions, the level of economic activity within the sector accounts for approximately 20.6% of economic activity within the wider financial services sector. At the end of 2023, total income within the banking sector was $161.7 million or approximately 10% of Gross Domestic Product (GDP), with net interest income standing at $238.62 million. Assets held were valued at $2.99 billion.

[55] 1373 transactions to and from Tier 1 countries, valued at $442,654 (0.83% of total transactions).
[56] 10,196 transactions to and from Tier 2 countries, valued at $2,701,261.
[57] One of the commercial banks is domestically owned with the majority shareholder being the Government of the Virgin Islands. The other five commercial banks are subsidiaries or branches of international banking groups established in jurisdictions that have been assessed as having equivalent AML/CFT regimes to the VI.

The banking sector predominantly provides banking facilities to local residents and businesses. However, the sector does provide services to non-resident persons, either directly or through the provision of banking services to LPLAs whose BOs and other associated relevant persons are non-resident within the Territory. Six of the seven licenced banks in the VI have clients resident in the VI whose nationality is of a Tier 1 or Tier 2 jurisdiction. A total of 13 of those clients are nationals of Tier 1 jurisdictions. An additional 74 clients are nationals of Tier 2 jurisdictions. A full breakdown is contained in the annex.

The products and services offered by these institutions are predominantly offered on a face-to-face basis and are relatively standard.[58] None of the banks within the VI offer prepaid card services. It has been found, based on international typologies, that wire transfers that support retail, commercial, wealth management, corporate and international transactions may be vulnerable to abuse. However, no such abuse has been detected in the VI domestic banking system. Foreign correspondent banking services are not provided by any bank in the Territory. However, with the exception of the one domestically owned banks, each bank has relationships with overseas banks that provide the local entities with correspondent banking services. Debit cards and wire transfers that support corporate and international transactions have been identified as being most susceptible to TF globally, yet none of the products and services offered by VI banking institutions are considered highly susceptible to TF given the client base to which these services are provided cross-border transactions primarily involve transfers to and from North America, Asia, the UK and the Caribbean. None of the banks reported any movement of funds to or from any Tier 1 of Tier 2 countries.

Most institutions offer some form of online banking; however, none of the banks in the VI use online platforms to onboard clients nor do they engage EIs for onboarding. A large proportion of business is still conducted face-to-face based on the institutions' infrastructure and the products and services offered. Thus, the delivery channels used are primarily face-to-face, including in relation to the on-boarding of clients, although there has been a gradual shift to more non-face-to-face transactions as online services have become more readily available within the sector. The FSC is not aware of any parent company or any directors etc. of any licenced bank that has links to Tier 1 and Tier 2 countries.

[58] Such services include Checking and savings accounts, credit cards, residential and commercial mortgages, auto and personal loans, time certificates of deposits, wire transfers that support retail, commercial, wealth management, corporate and international transactions.

SAR filing within this sector is commensurate with general expectations. Between 2022 and 2023, 330 SARs were received by the FIA. However, none of these SARs were TF related. The FSC carried out a thematic review of the SAR filings regime by the sector during 2022, which identified that proper procedures are in place, and that filings are commensurate with type/nature of clientele. The banking sector has robust systems in place and the FSC has not had cause to take any enforcement action for any AML/CFT related breach. FSC's analysis of the compliance officer reports, which are required to be submitted on an annual basis, demonstrates that banks are robustly training their staff and that AML/CFT awareness within the banking sector is at a high level, as evidenced by the training and testing conducted, as documented in the reports. There are no unregulated actors within the banking sector and there are no impediments to sharing information with the private sector.[59]

Table 1 – Banking Sector Vulnerabilities

Client Base	Product or Service	Distribution Channel	Other links to Tier 1 or Tier 2 countries	SAR filing	Implementation of CDD obligations/ internal controls	AML/CFT compliance and awareness	Scope of unregulated actors	Ability to share information with the private sector	Overall Vulnerabilities
L	L	L	L	ML	L	L	L	L	L

3.1.2 Money Service Businesses

MSBs in the VI are licenced and regulated under the Financing and Money Services Act, 2020 (as amended) (FMSA) and are legally obligated to adhere to the requirements set out in the Anti-Money Laundering Regulations, 2020 (as amended) (AMLRs) and the Anti-Money Laundering and Terrorist Financing Code of Practice (AMLTFCOP). There are only two MSBs licenced to operate in the VI and the level of economic activity within the MSB sector currently accounts for approximately 3.9% of economic activity within the wider financial services sector. The two licenced MSBs are part of large international money transfer

[59] In relation to the FSC and all supervised sectors, information is shared via direct communication with the licencees as necessary, along with various media including direct mailings, website postings, online videos, webinars, newsletter articles and the FSC's Meet the Regulator Forums. Types of information shared include updates on sanctions listings, public statements on potential fraudulent or unregulated activities, sectoral findings of onsite inspections, risk assessment findings, proposals for legislative changes, new filing requirements etc.

organisations with operations throughout the wider Caribbean region and beyond. Services are provided through two branches and three representative offices and are limited to money transfer services.

The core markets for MSBs within the VI are migrant workers repatriating funds to their home countries, and residents sending money abroad primarily for business and educational support purposes. Both MSBs currently service persons residing in the VI whose nationality is of a Tier 1 or Tier 2 jurisdiction. However, the percentage of these clients in relation to their overall client base is negligible. In 2023 these persons sent and received funds from Tier 1 jurisdictions. They also sent and received funds from Tier 2 jurisdictions.

At the end of 2023, MSBs recorded 1373 transactions to and from Tier 1 countries valued at $442,654 (0.83% of total transactions). For that same period, 10,196 transactions to and from Tier 2 countries were valued at $2,701,262 (or 5% of total transactions). Based on labour force data the level of remittances is commensurate with the current demographic composition of the local labour force. The jurisdictions in question equate to the country of origin of migrant workers who tend to repatriate funds to their home countries to support their families.

Furthermore, none of the MSBs use online platforms or EIs to onboard clients. No parent company or director etc. of any licenced MSBs has links to Tier 1 and Tier 2 countries.

In relation to the two licenced MSBs, one MSB has been risk-assessed as Medium-Low and the other Medium-High. Between 2022 and 2023, seven SARs were filed by the MSB rated as Medium-High. Three of these SARs were filed in 2022 and 4 in 2023. None of the SARs filed related to TF. Based on the 2020 TF and 2022 ML RAs the overall risk identified within this sector is Medium-Low. In addition, the nature of the transactions and clientele within the VI would not lead to a significant number of SARs. However, the current level of SAR filings is not considered commensurate with the risk posed by the sector given its cash intensive nature, which somewhat elevates the risk.

The sector is largely compliant with the implementation of CDD and other internal control mechanisms as evidenced through inspections and desk-based reviews. Inspection findings for the two MSBs reveal a rating of largely compliant as it relates to conducting CDD and verification on customers. There were few to no exceptions regarding CDD, as the established

controls require immediate CDD and verification prior to the conduct of any transactions. AML / CFT compliance and awareness within the sector is at a high level as evidenced by the results of onsite and desk-based monitoring and the FSC's analysis of the annual compliance officer reports which document the training and testing conducted by the licenced MSBs. In relation to unregulated actors for the MSB sectors, no such activity has been identified by the regulator. With respect to sharing information with the private sector, as described above for banking there are no impediments to sharing information.[60]

Table 2 – MSB Sector Vulnerabilities

Client Base	Product or Service	Distribution Channel	Other links to Tier 1 or Tier 2 countries	STR filing	Implementation of CDD obligations / internal controls	AML / CFT compliance and awareness	Scope of unregulated actors	Ability to share information with the private sector	Overall Vulnerabilities
ML	ML	L	L	ML	L	L	L	L	ML

3.1.3 Insurance[61]

The insurance sector in the VI consists of 45 domestic and 38 captive insurance companies, 6 insurance managers, 12 agents, 2 brokers and 3 loss adjusters. As of 31st December 2023, there were a total of 106 licences. Overall, the level of economic activity within the insurance sector accounts for approximately 3.9% of economic activity within the wider financial services sector.

No licencees have any clients resident in the VI whose nationality or residency or BO nationality or residency is of a Tier 1 jurisdiction. Five insurance licencees have 494 clients resident in the VI whose nationality or residency or BO nationality or residency is of a Tier 2 jurisdiction. This constitutes approximately 1% of the sector's client base. The current products offered by the insurance sector are not generally susceptible to TF abuse.[62] Further,

[60] See footnote above regarding means by which information is shared with the sector.
[61] Entities seeking to carry out insurance business in or from within the VI must be licenced under the Insurance Act, 2008.
[62] Property and casualty (homeowners, liability, fire and perils, builder's risk, business interruption, burglary) life and health (life policies, annuities, accidental, health) and marine (marine hull, cargo) insurance

no insurer or insurance intermediary uses online platforms or EIs to onboard clients. The FSC is not aware of any parent company or directors etc. of any licenced insurer or insurance intermediary having links to Tier 1 and Tier 2 countries.

Between 2022 and 2023, twelve SARs were filed by the insurance sector, none of which related to any TF or TFS activity. SAR filings are commensurate with risk within the sector, where most products in the domestic market are low risk and not susceptible to TF risk. The sector is largely compliant with the implementation of CDD and other internal control mechanisms as evidenced through inspections and desk-based reviews. FSC's analysis of training and testing conducted by the sector as outlined in the annual compliance officer reports confirms that AML/CFT compliance and awareness is at a high level within the insurance sector. There is no evidence that there is unregulated activity taking place in this sector and there are no impediments to sharing information with entities within the sector.

Table 3 – Insurance Sector Vulnerabilities

Client Base	Product or Service	Distribution Channel	Other links to Tier 1 or Tier 2 countries	STR filing	Implementation of CDD obligations / internal controls	AML / CFT compliance and awareness	Scope of unregulated actors	Ability to share information with the private sector	Overall Vulnerabilities
L	L	L	L	L	L	L	L	L	L

3.1.4 Investment Business[63]

All IB licences are subject to the Securities and Investment Business Act, 2020 (as amended) (SIBL) and the relevant regulations emanating from this, and licences may be granted in one or more categories to conduct various activities. In the VI, the IB sector includes six general categories: Investment Fund Vehicles, Asset and Investment Managers and Advisers, Brokers/Dealers, Asset and Investment Administrators, Custodians and Investment Exchanges. At the end of 2023, 230 entities held various categories of IB licences.

[63] To provide IB in or from within the VI, entities must be licenced by the FSC.

Investment management and advisory services make up the majority of the IB sector, with equity investments and shares making up the majority of assets held. In December 2023, investment funds registered in the VI had a total net asset value of approximately US$728 billion. However, the level of economic activity within the IB sector accounts for less than 5% of economic activity within the wider financial services sector in the VI.

The transactions involving this sector overall are significantly large, both in terms of the number of transactions and aggregate size of those transactions, with clientele geographically dispersed worldwide and engaging in cross-border transactions.[64] There is a rather small group of licencees (8) that provides custody services which is minimal and not consequential, given the limited number of transactions they execute.

At the end of 2023, twenty-seven IB licencees (mainly brokers (99%)) had clients whose nationality or residency or BO nationality or residency was of a Tier 1 or Tier 2 jurisdiction. Of those 27 entities, 14 licencees service 48,968 clients who are nationals of Tier 1 jurisdictions (all individuals except for one company), which accounts for 10% of those 14 licencees' client bases and 3.2% of the sector's total client base. In addition, 26 of the 27 licencees service 69,584 clients who are nationals of Tier 2 jurisdictions (111 companies and 69486 individuals). This accounts for 14% of the 26 licencees' client base and 4.6% of the total IB sector client base.

Of the products and services offered by IBs, transferable securities, mutual funds and derivative products are internationally recognised as being most susceptible to TF abuse[65]. 51 licencees or 11% of IBs offer derivative products (primarily offered by brokerage entities). Twenty-five IB licencees use online platforms for onboarding. With regard to the use of EIs, no IB licencees conduct business with EIs in any Tier 1 countries. However, licencees engage a small number of EIs from Tier 2 countries.

The FSC has not identified any parent company branch/subsidiary, directors etc. of any licenced IB with links to Tier 1 and Tier 2 countries.

[64] IB entities engage with regulated banks and the transactions are primarily fund, asset and securities trading.
[65] FATF Money Laundering and Terrorist Financing in the Securities Sector October 2009

Analysis of risk data shows associated risk primarily in the brokerage sub-sector. Other subsectors such as management of funds demonstrate a lower level of risk than brokerage services, given the clientele. Overall, SAR filings are generally considered low in comparison to the overall risk associated with the IB sector. Between 2022 and 2023 a total of 87 SARs were filed by licencees accounting for 5% of the IB sector.

Thirteen inspections were conducted during the period 2020 – 2022, with eleven inspections focusing on the level of implementation of CDD obligations. Results indicated that CDD obligations are carried out, as only three of the eleven licencees inspected received a rating less than largely compliant. All other IB licencees received a rating of Compliant or Largely Compliant, evidencing the establishment and implementation of appropriate CDD controls.

Analysis of AML/CFT returns data indicates a satisfactory level of awareness of AML/CFT measures. Some level of compliance is evident from onsite inspections as well with a majority of entities reviewed receiving a rating of Largely Compliant and Compliant as it relates to CDD and verification.

FSC's policing the perimeter has found that the scope of unregulated activity is limited.[66] Most investigations into unregulated activity reveal that identified activities are carried out by entities purporting to be VI entities but in fact are not registered, incorporated and/or have any connection to the Territory. The results of these investigations conducted between 2020 and 2023 revealed that fake licencees and bogus businesses fraudulently claiming to be authorised and licenced in the VI to conduct IB account for 11% of the total investigations. Public statements were issued on the FSC's website to alert the public about potential scams or fraudulent activities that may result in financial loss. Further, 13 investigations relative to complaints regarding IB Licencees were referred to the Supervisory Divisions. The basis for the complaints related to unresponsiveness of the licencees and matters concerning withdrawal policies. Only 4 of the 6 policing the perimeter investigations conducted between 2020 to 2023 involved BVIBCs. The other 42 involved non-BVIBCs purporting to be BVIBCs.

[66] It should be noted here that while the policing the perimeter activities involve looking for any signs of unauthorised business in any sector. The current findings relate to IBs and VASPs. This is generally consistent with international typologies where unauthorised banking, insurance and fiduciary business are rare.

There are no impediments with regard to sharing information with the IB sector.[67]

Table 4 – Investment Business Sector Vulnerabilities

Client Base	Product or Service	Distribution Channel	Other links to Tier 1 or Tier 2 countries	STR filing	Implementation of CDD obligations / internal controls	AML / CFT compliance and awareness	Scope of unregulated actors	Ability to share information with the private sector	Overall Vulnerabilitie
H	H	L	L	H	ML	ML	ML	L	ML

3.1.5 Financing

Under the FMSA, the definition of Financing Business (FB) includes the provision of a wide range of credit services including pay day advances, consumer finance loans under a financing agreement to a borrower in the VI, leasing property under financing lease agreements, cheque cashing and international financing and lending. Only FBs that operate physically in the VI are subject to authorisation and supervision. There are three licenced FBs in the Territory. Prior to Q2 2024 there were only two licencees, one of which serviced around 772 clients in 2023, executing approximately 408 transactions. The average value of the transactions was $2 million. Services provided are limited to small micro loans and short-term loans to persons within the organisations. The other licence conducted a total of 824 transactions in 2023 with an average value of $5,828 per transaction.

No licenced FB has clients who are nationals or residents, or whose BO is a national or resident, of any Tier 1 Tier 2 countries. Given the types of services provided, none of the products offered by FBs in the VI are vulnerable to TF abuse no do any FBs use online platforms or EIs to onboard clients. There are no branches or subsidiaries and none of the parent companies' directors etc. of any licencees have links to Tier 1 and Tier 2 countries.

[67] See footnote above regarding means by which information is shared with the sector.

The risk of TF within the financing sector, given its size and products offered, is extremely low. No SARs have been received from the financing sector within the reporting period. However, given the narrow focus of the sector, this is commensurate with risk and clientele. CDD and internal controls have been implemented, and desk-based reviews find that these systems are adequate and fit for purpose. AML/CFT compliance and awareness within the sector is at a high level as evidenced by training conducted. The FSC's analysis of the compliance officer reports demonstrates that FB licencees are robustly training their staff. In relation to unregulated active, there was one instance where an unregulated actor, who was identified and a fine issued. That entity has since been licenced. There are no impediments to sharing information with the sector.

Table 5 – Financing Sector Vulnerabilities

Client Base	Product or Service	Distribution Channel	Other links to Tier 1 or Tier 2 countries	STR filing	Implementation of CDD obligations / internal controls	AML / CFT compliance and awareness	Scope of unregulated actors	Ability to share information with the private sector	Overall Vulnerabilities
L	L	L	L	L	L	L	L	L	L

3.1.6 Insolvency

In order to accept an appointment as an administrator, administrative receiver, interim supervisor, supervisor, provisional liquidator, liquidator (other than in a solvent liquidation) or bankruptcy trustee, an Insolvency Practitioner (IP) must be licenced, as provided for under the Insolvency Act, 2003. Overseas IPs must be appointed jointly with a VI licenced IP in instances where such an appointment is required. IPs in the VI comprise mainly accountants and legal practitioners who are part of accountancy or law firms. Their legal obligations, including AML/CFT obligations, however, relate only to them in their personal capacities and are not transferred to the firms. In 2023, there were 29 fully licenced IPs (an increase from 27 in 2020). Between 2020 and 2023, 305 insolvency appointments were made. In the vast majority of cases, these appointments were related to the winding up/liquidation of non-regulated legal persons i.e., BVIBCs.

With regard to insolvency services, the client base may include international Politically Exposed Persons (PEPs) and businesses operating in high-risk jurisdictions (for ML or TF). However, the general nature of insolvency business not being on-going business makes the risk of the sector being used for any TF purposes extremely miniscule and may come primarily in the possibility of potential collusion between the IP and the client. However, there have been no reported instances where a BVI IP has been linked to any TF-related activity. Further, due to the nature of insolvency business, no IP uses online platforms or EIs to onboard clients.

Given the nature of insolvency services, the risk of TF within the sector is extremely low and SAR filings are commensurate with this level of risk. Between 2022 and 2023, IPs filed nineteen (19) SARs with the FIA, none of which related to any TF activity. There are no identified issues with implementation of CDD obligations / internal controls across the sector or with AML/CFT compliance and awareness within the sector. There are no impediments to sharing information with the sector. Unregistered activities are nonexistent given the requirements under the relevant legislation to be approved to deal with insolvent liquidations.

Table 6 – Insolvency Sector Vulnerabilities

Client Base	Product or Service	Distribution Channel	Other links to Tier 1 or Tier 2 countries	STR filing	Implementation of CDD obligations / internal controls	AML / CFT compliance and awareness	Scope of unregulated actors	Ability to share information with the private sector	Overall Vulnerabilitie
L	L	L	L	L	L	L	L	L	L

3.1.7 Virtual Asset Service Providers[68]

VASPs are registered under the Virtual Asset Service Provider Act **(VASPA)** which came into force in 2023. However, VASPs have been subject to AML/CFT requirements since December

[68] VAs are also posing increasing TF risks, including for fundraising by ISIL, Al Qaeda and right-wing extremist groups, although the vast majority of terrorist financing still takes place using fiat currency. Virtual Assets: Targeted Update on Implementation of the FATF standards, 2023

2022. Registration of VASPs began in 2024. Data provided on VASPs will, therefore, cover activity within 2024.[69]

As of Q4 2024, there had been 65 applicants for registration, 9 of which have been registered under the VASPA thus far. Nine applicants (all startups that had not yet launched) withdrew their applications and four applications were refused. Of the 43 applications pending decision, 33 are established entities subject to the transitional provisions and are currently undertaking business and 10 are new applicants which have not commenced business.[70]

The FSC understands and expects that numbers in relation to customers serviced and transaction sizes will be high and remains engaged with applicants to address deficiencies identified in policies and procedures as well as effectiveness for established business. Applicants have been required to submit responses related to their current book of business, outsourcing arrangements, risk management and AML provisions.

Current data from applicants suggests that there is significant activity related to VASP Exchanges and Custody emanating from the VI. Specifically, current data indicates that medium-sized custodians and exchanges operating from within the VI have over 5 million customers in each category.

Noting the elevated AML/CFT risk that VASPs pose to consumers and the jurisdiction's reputation, the FSC has prioritised the review and completion of VASPs who currently have a material portion of their client base in Tier 1 & Tier 2 jurisdictions as well as applicants that have filed a notable number of SARs.

Table 7: Categorisation of Virtual Asset Service Provider Applications Received by the FSC

VASP	VASP Custodian	VASP Exchange	Total

[69] The FSC remains engaged with applicants to address deficiencies identified in policies and procedures as well as effectiveness for established business. Applicants have been required to submit responses related to their current book of business, outsourcing arrangements, risk management and AML provisions.
[70] At the time of the risk assessment, it was anticipated that all applicants would be decided upon by the end of Q1 2025.

	X		3
		X	2
X			35
	X	X	17
X	X		1
X		X	4
X	X	X	3

54% of the applications received are solely VASP (not providing custody or exchange services) which tend to pose a lower level of risk than those that provide custody or exchange services. Thirty (30%) of applications are combined business models of VASP custodians and VASP exchanges or the trifecta of all three registration types. In relation to established VASPs seeking registration, 32 of the applicants were compliant or largely compliant with AML/CFT requirements, 19 were partially compliant and 4 were non-compliant. The 4 non-compliant established entities were refused in Q4 of 2024. For startups, 7 were compliant or largely compliant with AML/CFT requirements and 3 were found to be partially compliant.

In terms of scale, the size of current businesses operating in the VASP sector varies widely, ranging from small entities with around 20 clients that focus on specialised services such as staking and crypto asset financing, to large enterprises serving up to 200,000 clients. Larger entities are likely involved in a broader array of activities, including virtual asset custody and comprehensive trading platforms.

While the client base for a number of smaller VASPs is primarily dominated by institutional clients, including large financial entities such as banks, investment funds, pension funds, and insurance companies, retail clients, who are individual investors engaging in the virtual asset market for personal investment or speculative purposes, form a significant portion of the client base of the larger VASPs such as custodians and exchanges and therefore account for the majority of clients across all VASPs. High net worth individuals and institutions, such as family offices and private wealth management firms, as well as corporations like tech companies, fintech startups, and large enterprises seeking to diversify their balance sheets, also play a

substantial role. On the other hand, miners and traders, both professional and amateur, contribute to the client base to a lesser extent.

The FSC notes that a number of applicants operating from within the VI not only have a large client base, but also hold a significant market share within the global virtual asset space with 4 applicants ranking in the top 20 virtual asset exchanges globally, solely based on trading volume.

The products and services offered by VASPs that are most susceptible to TF include exchanges, Over-the-counter (OTC) services, VA wallets[71] and Non-Fungible Tokens (NFTs). A total of 25 VASPs have sought registration to operate as exchanges. From the responses thus far, 7 are offering OTC services and 2 are offering wallet services, and engaging in the sale of NFTs.

The number and value of transactions to and from or connected to Tier 1 and Tier 2 countries is currently unknown. Initial engagement with applicants indicates that a majority of applicants currently use online platforms for onboarding. At present, 4.4% of applicants have clients in Tier 1 and Tier 2 countries. There are currently no directors linked to Tier 1 countries. However, there are 12 directors currently linked to Tier 2 countries. There are also no parent companies linked to Tier 1 and Tier 2 countries.

The concentration of clients in both Tier 1 and Tier 2 jurisdictions (97%) is predominantly held across 3 applicants, 2 of whom are in the same VASP Exchange group. The FSC has identified 9,035 clients across ten of the twelve Tier 1 countries (none in Iran or Syria), approximately 90% of which were Nigeria and Pakistan and 77,309 clients across each of the nineteen Tier 2 countries. See Table 8 below.

Table 8 – Virtual Asset Service Provider Clients in Tier 1 and Tier 2 Jurisdictions

	No. of Clients in Tier 1	No. of Clients in Tier 2
Total Clients	9035	77989
Institutional clients	7	680
Retail clients	9028	77309

[71] Noting that providing a wallet is not a licensable activity and the higher risk is those opened not via licenced VASPs.

Currently there are fifteen VASPs with clients in Tier 1 and/or Tier 2 jurisdictions, eight of which have clients in Tier 1 jurisdictions. All fifteen have clients in Tier 2 jurisdictions. The number of companies with offerings in each high-risk jurisdiction is detailed below.

Table 9 - Companies Offering Virtual Asset Services in High-Risk Jurisdictions as of 31 December 2024

Tier 1 Distributions	
Jurisdictions	# of Companies with Offerings in each Tier 1 Jurisdiction
Afghanistan	1
Burkina Faso	4
Iran	0
Lebanon	3
Mali	3
Myanmar	2
Niger	3
Nigeria	7
Pakistan	6
Somalia	3
Syria	0
Yemen	3

Tier 2 Distributions	
Jurisdictions	# of Companies with Offerings
Algeria	4
Cameroon	4
Chad	3
Chile	9
Colombia	8
Democratic Republic of Congo	3
Egypt	5
Haiti	4
India	9
Iraq	1
Israel	9
Kenya	5
Mozambique	4
Palestine, State of	2
Philippines	9
Qatar	5
Saudi Arabia	7
Turkey	7
United Arab Emirates	9

Some larger applicants filed a notable number of SARs between 2022 and 2023. Of those applicants, the exchanges with a significant market-share filed roughly 3,952 SARs during 2022 and 5,860 during 2023, a Y-on-Y increase of 48%. The filings are consistent with the identified risk within the VASP sector but also indicative of adherence to the AML laws that came into effect on 1 December 2022, and continued application of AML screenings. Between 2022 and 2023, seven VASPs filed 83 SARs related to potential TF-related activity which speaks to this level of risk. The TF risk is elevated in this sector.

The FSC has taken steps to identify VASPs that are not registered or did not apply prior to the end of the 6-month transition period following the coming into force of the VASPA. Steps include investigations by the Enforcement Division (ED) and Specialised Supervision Unit (SSU). In one case a public statement was issued, and the entity was struck off and subsequently dissolved. In addition, the FSC has issued 46 public statements warning persons of various entities and individuals who have been found to be carrying out unauthorised business, including unauthorized VASP-related activities.[72] Between 2019 and April 2024, the FSC initiated investigations into 63 persons for fraudulent activities related to VAs activities. None of these related to TF. The Enforcement Division also investigated a total of 71 complaints/inquiries relating to 38 persons purporting to be registered/incorporated VI Companies or licenced entities with the FSC. None of these related to TF.

There are no impediments to sharing information with the private sector. Information is shared via various media including direct mailings, website postings, online videos, webinars, newsletter articles and the FSC's Meet the Regulator Forums. Types of information shared include RA findings, proposals for legislative changes, new filing requirements etc.

Table 10 – Virtual Asset Service Provider Sector Vulnerabilities

[72] These statements can be access at https://www.bvifsc.vg/library/alerts.

Client Base	Product or Service	Distribution Channel	Other links to Tier 1 or Tier 2 countries	STR filing	Implementation of CDD obligations / internal controls	AML / CFT compliance and awareness	Scope of unregulated actors	Ability to share information with the private sector	Overall Vulnerabilities
H	H	H	H	ML	MH	MH	MH	L	MH

Use of Virtual Assets[73]

In order to assess the use of VAs within the jurisdiction, the extent to which VAs were accepted by each of the regulated sectors outside of VASPs was considered[74] along with the prevalence of the use of VAs in the jurisdiction. An estimate was made on the number of users in the VI using open-source publications such as Chainalysis annual reports.

VAs are not used or accepted in the banking sector for general banking purposes. One bank provides services to persons in the VAs space but more so as holding capital on behalf of the VASP. Banks do not trade in or offer trading in VA. No FB currently use or accept VAs as a form of payment for services. IPs do not use or accept VAs as a form of payment for services. VAs are not used in the MSB sector or the insurance sector.

Based on the findings of the Risk Assessment Questionnaire for 2024, VAs are not accepted or used in the accounting sector, the real estate sector, the DPMS sector or the HVGD sector. Two entities provide virtual asset services in the capacity of legal advice. Outside of the VASP sub-sector, only a very limited number of IBs use or accept VA. No other sub-sector currently uses or accepts VAs as a form of payment for services.

Only a very limited number of IB brokers accept VA for payments and these payments constitute only 10% of total payments received by these brokers. No other sub-sector currently uses or accepts VAs as a form of payment for services except for the one licenced exchange

[73] Virtual assets are also posing increasing terrorist financing risks, including for fundraising by ISIL, Al Qaeda and right-wing extremist groups, although the vast majority of terrorist financing still takes place using fiat currency. Virtual Assets: Targeted Update on Implementation of the FATF standards, 2023

[74] The sector involves the trading and exchange of virtual assets such as Bitcoin, Ethereum and Tether.

which indicated that all payments are made via VAs as it provides services in relation to derivatives for VAs.

Prepaid payment cards are not available in the VI, nor are VAs accepted for public sector payments. However, there are few instances of acceptance of VA for payment in the private sector. The use of VA as a payment means in the VI is minimal. HMC has not received any declarations for cold wallets or mining equipment. There is, however, a growing number of BVIBCs that provide VASP services or involved with VAs, particularly cryptocurrencies.

Since June 2023, the GO has received an increase of reports of suspected/attempted sanctions breaches involving funds being transited through VI VASPs. This trend is being closely monitored by the GO, FIA and FSC and investigations regarding suspected involvement of VI VASPs in TF are underway. However, the majority of reports received involve the same BVIBC.

VAs and virtual asset platforms are attractive to terrorists because they provide a high level of anonymity that terrorists can exploit to move funds without detection. This makes it difficult for authorities to trace the identity of the individuals involved in the transaction as well as its purpose.

3.1.8 Trust and Corporate Service Providers

Since 1990, TCSPs have been classified as financial institutions and are licenced and regulated in accordance with the BTCA and the Company Management Act, 2020 (as amended) (CMA). In the VI, TCSPs fall into two general categories:

- Corporate Services Providers (CSPs)– these TCSPs engage primarily in company management and administration services including the provision of nominee shareholder and directorship services; and
- Trust Services Providers (TSPs) – these TCSPs engage in the provision of trustee and other related services to trusts.

At the end of 2023, 287 entities were licenced to operate under the BTCA or CMA in one of the six classes of licences. Of those 287 licenced TCSPs, 183 TCSPs are part of larger groups of companies operating either in other international finance centres where they are licenced or authorised, while 20 are part of larger groups operating locally. Nineteen CSPs are also

affiliated with legal or accounting firms operating within the Territory. Approximately 65 are independent operators.

Corporate Services Providers: At the end of 2023, 103 or 36% of the 287 TCSPs licenced in the Territory had the ability to provide company management services. This included provision of RA services to 340,796 BVIBCs who at the end of 2023 were active on the Companies Register (i.e., in good standing and in compliance with the BVIBCA), 2,042 active limited partnerships and 56 active foreign companies. Only CSPs that are categorised as RAs are permitted to incorporate or register legal persons. CSPs may also provide services such as directorship services and nominee shareholder services. A majority of all TCSPs (68%) have the ability to offer corporate director services. Further, 68% of all TCSPs have the ability to provide nominee shareholder services.

Trust Services Providers: At the end of 2023, 126 (or 44%) of the 287 TCSPs were licenced to provide trust related services, with 74 licenced exclusively to provide trust services. The latter accounts for 26% of all licenced TCSPs. At the end of 2023 there were 6,742 express trusts under administration by TSPs valued at approximately $171.08 billion. In addition, TSPs held 1,115 trusts under the VI Special Trusts Act, 2003.

Some companies that act as trustee or provide other trust related services, particularly for a group of related family trusts, are recognised as Private Trust Companies (PTCs) 75 and are exempted from the licencing requirement under the BTCA. At the end of 2023 there were 1,085 PTCs established in the VI. In June 2022, the FSC reviewed the level of compliance by relevant Class I licencees authorised to provide services to PTCs 76 and found they had adequate policies and procedures in place and were taking steps to risk assess these PTCs and monitor their ongoing compliance. Copies of trust documents for the trusts that PTCs act for were available at the TCSPs offices as required. It was also found that the majority of PTCs provide unremunerated services. PTCs, on average, provide services to less than two (1.3) trusts, which are generally family or related trust structures. The average Assets Under Management per trust

[75] A PTC is considered a relevant person for AML/CFT purposes and is required to comply with the AML Code, AML Regulations and all other relevant AML/CFT requirements in the VI.

[76] This was partially in relation to assessing whether these TCSPs had proper policies in place, had risk-assessed the PTCs, maintained the required documentation, and had proper measures in place to monitor the PTCs to get an understanding of the size of the PTC sector in terms of number of trusts for which they act, the services provided (i.e. unremunerated or related services) and to factor the findings into FSC's risk-based approach to supervision of these entities.

is approximately $13m. The data gathered was used to update the RAs of the relevant Class I TCSP licencees and increase the FSC's understanding of risk posed by PTCs and the legal arrangements they acted for.

One hundred and eleven TCSPs have clients whose nationality or residency, or whose BO's nationality or residency, is of a Tier 1 or Tier 2 jurisdiction. Those entities service 3317 clients who are nationals of Tier 1 jurisdictions and make up 0.07% of the total client base within the TCSP sector. These entities also service 31,795 clients who are nationals of Tier 2 jurisdictions, which make up 6.7% of the total TCSP sector client base. These clients are a combination of end users and clients engaged by way of third-party introductions.

Of the products and services offered by TCSPs incorporation services (offered by 36% of TCSPs), trust services (offered by 44% of TCSPs), and nominee services (offered by 68% of TCSPs) are most susceptible to TF abuse[77], in addition to Introduced Business Relationships which are used by 30% of TCSPs. No TCSPs use online platforms for onboarding. TCSPs do, however, engage a small number of EIs from Tier 1 and Tier 2 countries when onboarding clients (details in the annex). To the FSC's knowledge, no parent company, branch/subsidiary, directors etc. of any licenced TCSP have links to Tier 1 and Tier 2 countries.

Between 2022 and 2023, the FIA received 448 SARs from entities within the TCSP sector, of which 2 SARs, which were filed by the same TCSP, related to potential TF-related activity. Given the size of, and inherent risk within the TCSP sector[78], SARs filings are not commensurate with risk within the sector.

Implementation of CDD and internal controls across the sector is satisfactory but requires improvement though entities generally have controls in place. For the period 2020 – 2023, TCSPs were generally compliant with the requirement to undertake CDD and inquire into the circumstances of the customer. Specifically, during 2020 – 2023, Six CSPs were assessed for CDD, and all received a rating of Largely Compliant. Regarding EDD, there were fifteen inspections conducted which assessed licencees' effective implementation of their EDD procedures, of which twelve TCSPs demonstrated deficiencies. Of the 12, Nine TCSPs (60%)

[77] The Misuse of Corporate Vehicles, Including Trust and Company Service Providers, FATF, 13 October 2006
[78] Previously assessed as Low for domestic TF and Medium-Low for foreign TF.

were rated as Partially Compliant whilst three TCSPs (20%) were rated as non-compliant. The remaining three TCSPs (20%) had minor or no deficiencies.[79]

AML/CFT awareness within the sector is high. Data from Compliance Officer reports and other desk-based reviews show continuous training and development. Onsite inspections generally find training is undertaken as required. Additionally, no unregulated activities have been discovered as, given the services provided and the fact that all entities require an agent to be incorporated, unregulated activity in this sector is generally unlikely.[80] There are no impediments to sharing information with the private sector.[81]

Table 11 – Trust and Corporate Service Provider Sector Vulnerabilities

Client Base	Product or Service	Distribution Channel	Other links to Tier 1 or Tier 2 countries	STR filing	Implementation of CDD obligations / internal controls	AML / CFT compliance and awareness	Scope of unregulated actors	Ability to share information with the private sector	Overall Vulnerabilities
MH	H	L	L	H	MH	ML	L	L	MH

3.1.9 Accountants

In 2023, there were 18 registered accountants, of whom 7 were also licensed IPs and 5 were registered accounting firms which engage in general accounting activities such as auditing and not relevant business. The remaining 6 conducted relevant financial business in accordance with the AMLTFCOP, which made them subject to AML/CFT supervision by the FIA. The sum value of the transactions conducted by these six registered accountants for 2023 was $287,277,673, for those also carrying out insolvency business the sum value of transactions conducted for 2023 was $1,779,656,509.73.

Out of the total client base there were no clients from Tier 1, there were 2 from Tier 2 (UAE). One entity had a BO from Tier 1 (Pakistan) and 2 entities had BOs from a Tier 2 country

[79] 2 were largely compliant and 1 was compliant.
[80] Given the services provided and the fact that all entities require an agent to be incorporated, unregulated activity in this sector is generally unlikely.
[81] For methods of how the information is shared see the footnote above regarding banking.

(Philippines). Wire transfers and checks are the main methods of payment used by the sector. Between 2021 and 2023 10 SARs were filed by 3 entities which is commensurate with its risk given the size and nature of the sector..

A total of 90% of the accountants have written AML/CFT/CPF compliance programmes. Some of these firms form part of larger international firms with established business relationships across the globe. In relation to those accountants who are insolvency practitioners, there are no identified issues with implementation of CDD obligations/internal controls nor with AML/CFT compliance and awareness according to FSC. Between September 2024 – October 2024, FIA-SEU conducted and concluded onsite inspections on two accounting firms for the period 2021 – 2023. Each accountant received a rating of partially compliant with the requirement to undertake appropriate and adequate risk-based CDD and ECDD measures. This was due deficiencies in the conduct of their institutional / customer risk assessment and their ability to accurately identify risk and apply the appropriate mitigating measures. AML/CFT policies and procedure were in place but were not sufficiently risk-based and tailored to commensurate with the risks of the entities due to the deficiencies identified in institutional / customer risk assessment. However, there are general measures such as screening, monitoring and reporting in place to mitigate TF risk. The entities have a general understanding and knowledge of their AML/CFT obligations but there is room for improvement.

In relation to unregulated actors, accountants that engage in the relevant activities are registered.[82] registration is an ongoing process as new businesses are licenced with the Ministry of Trade daily. In relation to all its supervised sectors, the FIA-SEU, in an effort to ensure that all relevant businesses are registered with the FIA (a) issues an annual notice reminding entities of their obligation to register with the FIA once they are engaging in the relevant business and, (b) engages in "policing the perimeter" exercises in which, based on the list of licenced entities submitted by the Ministry of Trade, the FIA-SEU contacts new or existing entities to verify whether they are conducting the relevant activities and , if so, require that they complete and submit the relevant forms and supporting documents for registration purposes. It is therefore possible that there are new entities operating who are not yet registered for a very temporary period. All efforts are made to ensure entities conducting relevant

[82] The Ministry of Trade periodically provides a list of entities that are licenced and engaging in the relevant activities to the FIA-SEU (accounting, lawyers and notaries, real estate agents, DPMS and HVGD).

activities are registered. To date the FIA has not identified any accountants operating without authorisation and therefore no action was taken for failure to register.

There are no barriers for the sharing of information with the private sector. The FIA-SEU provides guidance and training to the accounting sector and communicates effectively via email and telephone. Whenever the FIA-SEU receives a new sanction listing it is immediately sent out to the entire DNFBP sector. As it is usually the Money Laundering Reporting Officers (MLROs) or the compliance team who are responsible for reporting sanctions breaches, the FIA SEU also liaises with these persons regarding sanctions breaches to keep them abreast of any new designation.

Table 12 – Accounting Sector Vulnerabilities

Client Base	Product or Service	Distribution Channel	Other links to Tier 1 or Tier 2 countries	STR filing	Implementation of CDD obligations / internal controls	AML / CFT compliance and awareness	Scope of unregulated actors	Ability to share information with the private sector	Overall Vulnerabilities
L	L	L	L	L	MH	ML	L	L	L

3.1.10 Lawyers and Notaries

In 2023, there were 36 registered entities which related to a sum value of $33,262, 227,558.50 in transactions conducted for 2023. One entity had clients in a Tier 1 country, 11 entities had clients in Tier 2 countries. There were no BOs related to Tier 1 or Tier 2 countries. There was one investigation involving a lawyer's client, but the lawyer was not conducting relevant financial business. Wire transfers and checks are the main methods of payment accepted. There are negligible cash transactions accepted. A total of 26 of the entities use online platforms for onboarding. No entities have links to Tier 1 and Tier 2 countries through affiliations or offices.

Between the years 2021- 2023, only 35 SARs were filed by 8 entities. This is not commensurate with risk given the size of, and inherent risk within the Legal sector.

96% of the firms possess a written AML/CFT/CPF compliance programme. Additionally, the VI has established global firms who have long-standing offices within the Territory and as such, have in place global compliance policies, procedures, control and systems to ensure compliance with AML/CFT regulatory requirements.

Registration is an ongoing process as new businesses are licenced with the Ministry of Trade frequently. The FIA-SEU, in an effort to ensure that all relevant businesses are registered with the FIA, takes relevant steps as outlined above for accountants. 9 new legal practitioners were recently registered with the FIA-SEU and attended the new registrant webinar on 18 February 2025. Measures are taken to ensure that all entities conducting the relevant activities are registered with the FIA.
The FIA has not identified any lawyers operating without authorisation and therefore, no action has been taken for failure to register.

There are no barriers for the sharing of information with the private sector. The FIA-SEU provides guidance and training to the legal practitioner sector and communicates effectively via email and telephone. The FIA-SEU sends sanctions updates immediately to all DNFBP sectors as well as liaises periodically with the MLROs via email to keep them abreast of any new designations.

Between September 2024 and October 2024, the FIA-SEU conducted onsite inspections on ten firms for the period 2021 – 2023. 7 of the entities received a largely compliant rating for undertaking appropriate and adequate CDD and ECDD measures which are risk-based. The three remaining entities received partially compliant mainly due deficiencies in the conduct of their institutional / customer risk assessment and their ability to accurately identify risk and apply the appropriate mitigating measures. Additionally, the onsite examinations and desk-based reviews further found that the international/global law firms are compliant with their CDD obligations and have implemented adequate and effective internal controls to mitigate risks, especially in relation to TF risk as there are robust systems in place which facilitate sanction screening, monitoring and reporting. Further, these firms are very aware of their AML/CFT obligations as they are part of global firms and have comply with international standards. However, while the smaller local law firms have some deficiencies in their general AML/CFT framework, they have some internal controls in place. These local firms have a general understanding of their AML/CFT obligations.

Table 13 – Lawyers and Notaries Vulnerabilities

Client Base	Product or Service	Distribution Channel	Other links to Tier 1 or Tier 2 countries	STR filing	Implementation of CDD obligations / internal controls	AML / CFT compliance and awareness	Scope of unregulated actors	Ability to share information with the private sector	Overall Vulnerabilitie
MH	MH	ML	ML	MH	ML	ML	L	L	ML

3.1.11 Real Estate Agents

In 2023, there were 13 registered Real Estate Agents (REAs) involving transactions whose sum value was $59,424,037 million. There were no clients, BOs or other links to Tier 1 or Tier 2 countries. There was one international typology in relation to the sale of real estate for TF purposes, however given the strict limits on such purchases in the VI[83] this was excluded. Wire transfers, cheques, cash and bank financing are the main payment methods accepted by the real estate sector. Between the years 2021- 2023, only 1 SAR was filed by 1 entity, which is below what would be commensurate with risk.

In 2024, the FIA-SEU conducted an onsite inspection on four real estates for the period 2021 – 2023. Each entity received a rating of partially compliant with the requirement to undertake appropriate and adequate risk-based CDD and ECDD measures. This was due deficiencies in the conduct of their institutional / customer risk assessment and their ability to accurately identify risk and apply the appropriate mitigating measures. Additionally, the AML/CFT policies and procedure in place, were not risk-based and tailored to be commensurate with the risks of the entities due to the deficiencies identified in institutional / customer risk assessment. However, there are general measures such as screening and reporting in place to mitigate TF risk. Most of the entities have a general understanding and knowledge of their AML/CFT obligations but there is much room for improvement.

[83] Foreign persons seeking to purchase property must apply for a licence (non-belonger land holding licence, 'NBLHL') which takes between three and nine months to obtain and consists of stringent requirements.

In relation to unregulated actors within the real estate sector, most of the REAs that engage in the relevant activities are registered with the FIA. As with other DNFBP sectors registration is an ongoing process as new businesses are licenced with the Ministry of Trade daily. The FIA-SEU issues an annual notice and engages in policing the perimeter abased on the list of licenced entities, the FIA-SEU contacts new or existing entities to verify whether they are conducting relevant activities and, if so, requires the relevant forms to be completed. Additionally, some entities contact the FIA-SEU for information regarding registration. The Ministry of Trade periodically provides a list to the FIA-SEU of entities that are licenced and engaged in the relevant activities to the FIA-SEU.

There are limited barriers to the sharing of information with the private sector. The FIA-SEU provides guidance and training to the Real Estate sector and communicates effectively via email and telephone. The FIA-SEU also sends sanctions listings periodically to the MLRO or designated person of the REA via email to keep them abreast of any new designation.

Table 14 – Real Estate Vulnerabilities

Client Base	Product or Service	Distribution Channel	Other links to Tier 1 or Tier 2 countries	STR filing	Implementation of CDD obligations / internal controls	AML / CFT compliance and awareness	Scope of unregulated actors	Ability to share information with the private sector	Overall Vulnerabilitie
L	ML	L	L	MH	MH	ML	L	L	ML

3.1.12 Dealers in Precious Metals and Stones

In 2023 there were 5 registered DPMS, with total revenue of $1,607,389. None of these entities has clients in Tier 1 or Tier 2 countries. Two entities had beneficial owners in a Tier 2 country (India and Israel although no longer residing there and one BO out of the five resided in the VI). There was no evidence to suggest any movement to or from Tier 1 or Tier 2 countries or connection with Tier 1 or Tier 2 countries. Additionally, there were no suppliers in Tier 1 or Tier 2 countries or any links to TF.

Between the years 2021- 2023, no SARs were filed by the DPMS sector (although one SAR was filed in 2024) which is not commensurate with the risk within the sector.

In 2024, the FIA-SEU conducted an onsite inspection on four DPMS for the period 2021 – 2023. Each entity received a rating of partially compliant with the requirement to undertake appropriate and adequate risk-based CDD and ECDD measures. This was due deficiencies in the conduct of their institutional / customer risk assessment and their ability to accurately identify risk and apply the appropriate mitigating measures. Additionally, the AML/CFT policies and procedures in place, were not risk-based and tailored to the risks of the entities due to the deficiencies identified in institutional / customer risk assessment. However, there are general measures such as screening and reporting in place to mitigate TF risk. Therefore, most of the entities have a general understanding of their AML/CFT obligations, but further training and guidance are required to foster better understanding of their AML/CFT obligations and risks. General AML / CFT training was undertaken but needed to be more specific in the area of TF.

In relation to unregulated actors within the sector, most of the DPMS that engage in the relevant activities are registered with the FIA-SEU. In addition, the Ministry of Trade periodically provides the FIA-SEU with a list of entities that are licenced and engaging in the relevant activities to the FIA-SEU. The FIA-SEU issues an annual notice to remind entities of the obligation to register and also policies the perimeter based on the list of licenced entities submitted by the Ministry of Trade. The FIA-SEU contacts new or existing entities to verify whether they are conducting relevant activities and, if so, requires that they complete and submit the relevant forms and supporting documents for registration purposes. The FIA-SEU has not identified any entities operating without authorisation and therefore, there was no action taken for failure to register. There are no barriers for the sharing of information with the private sector. The FIA-SEU provides guidance and training to the DPMS sector and communicates effectively via email and telephone. The FIA-SEU sends sanctions listings periodically to the MLRO of the DPMS via email to keep them abreast of any new designation.

Goods in the VI are primarily imported from the US mainland. There has also been an increase of importation of goods from China but none from high-risk TF countries. There has never been an interception of goods destined for high-risk countries where such goods were being transited through the VI.

In 2021 jewellery originating from Israel was imported from the US to the VI seven times being carried by a passenger on a ferry with US customs declarations forms. Other goods originating from Pakistan were imported through the airport. HMC reviewed these matters and confirmed there was no link to TF. In relation to the movement of precious metals, the route used appeared to be from the USA to VI onwards to St. Martin. There was no suspected link to TF. Neither the FCU nor the FIA-AIU had received any intelligence from any source relating to the movement of precious metals or stones for the purposes of TF. As such, the RVIPF FCU has conducted no investigations in relation to the movement of PMS. In relation to the movement or smuggling of goods including cash, BNIs and PMS The RVIPF IU received no information or intelligence relating to TF. Furthermore, there was no intelligence in relation to significant links to Tier 1 or Tier 2 countries or TF or terrorism. No vessels were registered to a legal owner in a Tier 1 or Tier 2 country or had any links to terrorism or TF.

Therefore, in relation to the movement of goods and the movement of PMS there has been no suspicion of, or information in relation to, TF

Table 15 – Dealers in Precious Metals and Stones Vulnerabilities

Client Base	Product or Service	Distribution Channel	Other links to Tier 1 or Tier 2 countries	STR filing	Implementation of CDD obligations / internal controls	AML / CFT compliance and awareness	Scope of unregulated actors	Ability to share information with the private sector	Overall Vulnerabilitie
ML	L	L	ML	MH	MH	ML	L	L	ML

3.1.13 High Value Goods Dealers

In 2023 there were 13 registered entities consisting of 6 car dealers whose sum value of transactions conducted for 2023 was $17,974,995.10 and 6 yacht brokers & 1 other high value goods such as machinery who conducted transactions in 2023 to a sum value of $13,702,984.80. 2 entities have clients / suppliers in Tier 2 countries. 1 entity has a BO based in a Tier 2 country.

No products or services were identified in relation to the use of the HVGD sector to facilitate TF. Wire transfer, cheques and bank financing are the main methods of payment used by HVGD.

Between the years 2021- 2023, no SARs were filed by the HVGD sector which is not commensurate with its risk.

In 2024, the FIA-SEU conducted an onsite inspection on two HVGD for the period 2021 – 2023. Each entity received a rating of partially compliant with the requirement to undertake appropriate and adequate risk-based CDD and ECDD measures. This was due deficiencies in the conduct of their institutional / customer risk assessment and their ability to accurately identify risk and apply the appropriate mitigating measures. Additionally, the AML/CFT policies and procedure were in place, but were not risk-based and tailored to the risks of the entities due to the deficiencies identified in institutional / customer risk assessment. However, there are general measures such as screening and reporting in place to mitigate TF risk. Therefore, most of the entities have a general understanding of their AML/CFT obligations, but further training and guidance are required to foster better understanding of their AML/CFT obligations and risks. Training in AML / CFT was also generic.

Most of the HVGD that engage in the relevant activities are registered with the FIA. New entities apply to the Ministry of Trade frequently and the FIA-SEU polices the perimeter. There are no barriers to the sharing of information with the private sector. The FIA-SEU provides guidance and training to the HVGD Sector and communicates effectively via email and telephone. The FIA-SEU sends sanctions listings upon receipt to the HVGD sector.

Table 16 – High Value Good Dealer Vulnerabilities

Client Base	Product or Service	Distribution Channel	Other links to Tier 1 or Tier 2 countries	STR filing	Implementation of CDD obligations / internal controls across the sector	AML / CFT compliance and awareness within the sector	Scope of unregulated actors	Ability to share information with the private sector	Overall Vulnerabilitie
ML	L	ML	L	MH	MH	ML	L	L	ML

3.2 Vulnerabilities – All Regulated Sectors

Table 17 - Summary of Vulnerability Ratings for Regulated Sectors

	Client Base	Product or Service	Distribution Channel	Other links to Tier 1 or Tier 2 countries	STR filing	Implementation of CDD obligations / internal controls	AML / CFT compliance and awareness within the sector	Scope of unregulated actors	Ability to share information with the private sector	Overall Vulnerabiliti
Banking	L	L	L	L	MH	L	L	L	L	L
MSB	ML	ML	L	L	MH	L	L	L	L	ML
Insurance	L	L	L	L	L	L	L	L	L	L
Investment Business	H	H	L	L	H	ML	ML	ML	L	ML
Financing	L	L	L	L	L	L	L	L	L	L
VASPs	H	H	H	H	MH	MH	MH	MH	L	MH
TCSPs	MH	H	L	L	H	MH	ML	L	L	MH
Insolvency	L	L	L	L	L	L	L	L	L	L
Accountants	L	L	L	L	L	MH	ML	L	L	L
Lawyers/ Notaries	MH	MH	ML	ML	MH	ML	ML	L	L	ML
DPMS	ML	L	L	ML	MH	MH	ML	L	L	ML
Real Estate Agents	L	ML	L	L	ML	MH	MH	L	L	ML
HVGDs	ML	L	ML	L	MH	ML	ML	L	L	ML

3.3 The Vulnerability of Non-Profit Organisations to Terrorist Financing as Sector[84]

The targeted NPO RA which was finalised in August 2024 and took into consideration variables such as, inter alia, the value of income/revenue, scale of operations, level of accountability required by funding sources, level of verifiability of fund-raising methods and level of cash transfers were considered. The VI engaged with the financial sector to fully understand the NPO sector, to determine the level of TF risk based on their financial activities

[84] 2024 Virgin Islands Non-Profit Organisation Terrorist Financing Risk Assessment

and to reduce the occurrence of de-risking, where necessary. A total of 95 NPOs and 7 banks actively participated in this assessment by completing and submitting a RA questionnaire.

For the period 2023, there were 121 registered NPOs in the VI which provided religious, charitable, social, environmental, educational, health, cultural, sports and animal welfare services.[85] 96% of the NPOs fell under the FATF definition of NPOs while 4% of the NPOs are deemed as non FATF NPOs.

Table 18 - Total Number of FATF Defined Non-Profit Organisations[86] Registered in the Virgin Islands in 2023

FATF Defined NPOs	**Number**	**Percentage**	
Religious	46	39.3	
Charitable	6	5.1	
Social	23	19.6	
Environmental	4	3.4	
Educational	10	8.5	
Health	5	4.3	
Cultural	5	4.3	
Sports	16	13.7	
Animal Welfare	2	1.7	
Total	**117**	**100**	

In 2023, the NPO sector generated a significant annual revenue of $38,001,984.35 million (USD). It was noted that the majority of the NPOs estimated annual income/revenue was under $50,000. However, 6 NPOs had a gross annual income/revenue of over $1,000,000. These are

[85] The NPO Risk Assessment also highlighted that the significance of NPOs should not be overlooked as they contribute significantly to the socio-economic development of the VI particularly in a period of unprecedented natural disasters such as Hurricanes Irma and Maria which caused widespread destruction across the British Virgin Islands in 2017.

[86] *A legal person or arrangement or organisation that primarily engages in raising or disbursing funds for purposes such as charitable, religious, cultural, educational, social or fraternal purposes, or for the carrying out of other types of "good works"* The Interpretive Note to Recommendation 8 (International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation – The FATF Recommendations 2023)

larger NPOs with international affiliations and donorship mainly from the US and the UK from reputable International Organisations.

Approximately 78% of the NPOs in VI are predominantly domestic in nature in that funds are raised and disbursed locally, while 22% engaged in cross-border activities such as the raising or disbursing of funds internationally. However, most of these activities are conducted predominantly in jurisdictions such as the US, UK, Europe and the Caribbean region. Twenty-six NPOs indicated that they received funds / donations from international organisations/ bodies. The largest cross-border funding was received by charitable and environmental NPOs: (a) from jurisdictions such as the UK and the US, which have been found to comply with the FATF standards through the implementation of various CFT legislation, policies and procedures[87] (b) mainly from reputable and known organisations; and (c) for projects and development in the VI and not transmitted or distributed internationally[88] which significantly reduces the TF risk given the lack of domestic terrorism in the VI.

Twenty-seven NPOs indicated that they disburse funds internationally (a) to jurisdictions such as the US, UK, Norway, Anguilla, St. Vincent, Ghana and Dominica, which have been found to comply with the FATF standards through the implementation of various CFT legislation, policies and procedures and do not present a high risk[89] (b) to reputable international organisations; and (c) the largest distribution was mainly for project procurement purposes such as equipment and services from international vendors in US and Canada. Although the disbursement of funds for humanitarian purposes presents a level of TF risk, based on the data collected, only a few NPOs provide humanitarian assistance internationally, which is mainly provided to low-risk jurisdictions in times of natural disasters and destitution, and rarely in areas with a high level of TF risk exposure.

Based on this analysis, it was concluded that FATF NPOs engaging in service activities are deemed most "at risk" for TF in the VI due to their level of cross border activities and foreign

[87] These jurisdictions have committed to the FATF Recommendations through the global network of FSRBs and FATF memberships and seek to comply with the FATF Recommendations and Standards. See: https://www.fatf-gafi.org/countries/

[88] Only for project procurement purposes such as equipment and services from international vendors in the US and Canada

[89] These jurisdictions have committed to the FATF Recommendations through the global network of FSRBs and FATF memberships and seek to comply with the FATF Recommendations and Standards. See: https://www.fatf-gafi.org/countries/

affiliation and control. Four service focused NPOs in the VI were assessed as high risk for TF due to their cross-border activities, affiliation and control in connection with high-risk jurisdictions. While there exist inherent vulnerabilities within the NPO sector and deficiencies in the legislative framework, the overall inherent risk is assessed as low due to the low level of TF threat and abuse.

3.4 The Vulnerability of Legal Persons and arrangements to Terrorist Financing in the Virgin Islands

Utilising the targeted risk assessment of LPLAs conducted in the VI in 2024, the findings were used to determine the vulnerability rating of LPLAs to TF in the VI. The TF high risk jurisdiction list confirmed by the TF WG was utilised in assessing the TF risk of the LPLAs to ensure consistency. It found that the highest vulnerability was posed by BVIBCs limited by shares (Medium-High), which constitute the overwhelming majority of LPLAs in the jurisdiction. In addition, BVIBCs limited by shares have by far the highest number of corporate directors. Legal persons, including limited partnerships, can have bodies corporate as their shareholders or, in the case of partnerships, their partners. These shareholders or partners can be from any jurisdiction in the world. These features increase the potential for opacity and dissimulation of BO thereby increasing the vulnerability of these legal persons to being misused for financial crime. There are 14,757 PEPs who are a BO of a legal person.[90] In addition, one PEP can be a BO for more than one entity. As such, the data shows that approximately 4% of legal persons have a BO that is a PEP.

Table 19 - Vulnerability Scores for Legal Persons and Legal Arrangements[91]

Type of Legal Person or Arrangement	Score
BVIBC - Limited by Shares	MH
BVIBC - Limited by Guarantee (shares)	MH
BVIBC - Limited by Guarantee (non-shares)	MH
Unlimited Company	MH
Unlimited company (non-shares)	MH

[90] While, this data is not broken out by type of legal person, this is not seen as a large data gap given that BVIBCs make up over 97% of all the legal persons in the VI.
[91] Table 9 of the VI LPLA Risk Assessment 2025

Segregated Portfolio Company	MH
Restricted Purpose Company	MH
Private Trust Company	ML
Limited Partnership	MH
International Partnership	MH
Partnership without Legal Personality	MH
Foreign companies	ML
Vista Trusts	MH
Express Trusts	MH

Data gaps about the nature of business carried out by VI legal persons remain, as the information captured in the current li TCSPs' annual return is very general. Requiring legal persons themselves to notify the Registrar of Corporate Affairs (ROCA) of their nature of business could yield more information. As a result, legal persons, other than foreign companies (low) and PTCs (Medium-Low), score Medium-High on this factor for TF. The LPLA RA found that 7% of legal persons have BOs in a high-risk jurisdiction for TF. Legal arrangements were found to be vulnerable to misuse due to the size of the sector and the links to high-risk jurisdictions for TF and the overall vulnerability was Medium-High.

Table 20 – Foreign Directorships of BVIBCs

Type of Directorship	**TF**
Limited by Guarantee- Authorised to issue shares	3.6% (Tier 2 countries)
Limited by Guarantee – Not authorised to issue shares	1.8% Tier 1 5% Tier 2
Unlimited Company	5% Tier 2
Company Limited by Shares	0.7% Tier 1 7% Tier 2

Data on the regions where VI legal persons operate is available in aggregate. However, data related to specific countries was not available.

The ease with which a legal person can be set up may increase the vulnerability to misuse of legal persons in a jurisdiction. In the VI, all types of legal persons can be incorporated within 24 hours. Regulatory requirements that legal persons must comply with at the time of incorporation include, for example having minimum capital, a minimum number of shareholders, having a VI resident director or a minimum number of directors. Only PTCs have

a more difficult set up process, as they must appoint a Class I trust license holder, in the VI refers to the highest level of TCSP license category, as its registered agent. All legal persons are incorporated via a TCSP. Moreover, the ability to establish a legal person is advertised internationally. Given these features, all types of legal persons except PTCs are rated as highly vulnerable on this factor and PTCs are rated as Medium-High.

The overall vulnerability score was Medium-High for all LPLAs except for PTCs and foreign companies. As above, given the small materiality of these two sub-sectors in comparison with BIVBCs limited by shares, the MH rating was used in this RA.

3.5 The Vulnerability of the Use of Cash and Bearer Negotiated Instruments in the Jurisdiction

The other area that was considered in terms of vulnerability to the VI was the use of Cash and BNIs. Given that the VI is generally a cash-based society, the risk of cash being misused for the purposes of TF was considered by assessing the frequency of the use of cash within the regulated sectors, cash seizures by law enforcement within the jurisdiction and at its borders and intelligence relating to the misuse of cash. This was then considered in terms of any potential vulnerability to TF.

Although the use of credit and debit cards for payments is becoming increasingly common as most businesses now have the ability to provide for such payment methods cash is still preferred. Particularly by smaller businesses where the number and/or value of daily transactions may not make it economically feasible to justify the processing fees associated with the use of debit and credit cards.

The total amount of cash seized by authorities in the VI both for failure to declare and for cash found in relation to criminal conduct is depicted in the table below. None of these matters had any nexus to TF.

Table 21 – Total Cash Seizures Over the Review Period

Year	2020	2021	2022	2023

Total Cash Seizure by FCU/RVIPF	1,515,726	927,975.47	657,856	147,476.00
HMC/RVIPF joint operations	878,566	322,723.49	19,100	0

Although substantial amounts of cash were seized over the specified years, indicative of potential proceeds of crime and money laundering activities, there is no indication that the cash seized is connected to TF.

Cash Based Businesses were defined as barber shops, hair and beauty salons, bus and tax services, car rental businesses, car wash businesses, laundromat and dry cleaners, jewellery stores, motor vehicle dealerships and nail salons. The total number of trade licences issued by the Department of Trade to these business types was 2684. Intelligence suggests that these businesses may be more susceptible to the facilitation of ML. However, no TF-related disseminations were made to the FCU as it relates to these businesses. These cash based small businesses are owned by Virgin Islanders and expatriates alike, for example, car and boat rentals, restaurants, car washes, beauty salons, mini supermarkets, and clothing stores are owned by Virgin Islanders and expatriates alike. While some of the owners are originally from high-risk jurisdictions such as Lebanon and Palestine, there is no evidence to suggest that cash earned through these businesses has been misused to facilitate TF.

No cash was seized from any cash intensive businesses. The total amount of cash seized overall for the relevant period was 3, 302,795 by RVIPF and $1,205,310 by HMC. None of which was found to have any link to terrorism or TF. In relation to cash coming in from higher risk countries the total noted by HMC was $78.646, none of which had any link to terrorism or TF. No cash was sent out to higher risk countries. The FIA-AIU indicated there was one SAR potentially linked to 4.46 million in cash which was categorised as ‘terrorism’ or ‘TF’. This related to a Tier 1 country. This matter was disclosed to the FCU and is under investigation.

Within the financial services sector, banking and MSBs licencees are considered the most cash-intensive business as these entities are the primary recipients of the cash generated by the wider economy. However, based on the services provided by these sectors the risk of misuse for TF is low. In banking cash is primarily limited to the receipt of deposits from individual account holders. Banks themselves have indicated that their preferred method to receive payments is through direct debit from a customer's account or via cheque or wire transfer. Verification of source of funds is conducted on over-threshold transactions. In some institutions the over-threshold limit requiring enquiry into source of funds and source of wealth is lower than the statutory limit of $10,000. Between 2020 and 2023 less than 4% of payments received were cash based.

Generally, the cash-intensive nature of the MSB sector, and the size of the annual value of outgoing and incoming transactions are factors that may impact the level of TF risk within the sector. In the VI outward money transfers constitute the greatest number of transactions recorded, accounting for 87% of all transactions at the end of 2023 valued at approximately $46.66 million. The average value of outgoing transactions is $569.25. Conversely incoming transfers were valued at $6.89 million at the end of 2023 or roughly 13% of all transactions. The average value of incoming transactions is $857.00. Given the demographic composition of the Territory, this imbalance between incoming and outgoing transfers is not unexpected. The use of cash for payment of services to MSBs varies, and averages approximately 13% of payments received, while cheques and credit/debit card payments account for approximately 63% and 14% respectively. While the use of cash within the MSB sector varies, money transfers to and from Tier 1 and Tier 2 jurisdictions constitute less than 6% of total transfers.

The use of cash for payment of services to insurers is limited, however, cash is widely accepted amongst intermediaries, being the preferred method to receive payments for services provided to clients. The percentage of total payments received via cash by intermediaries represents approximately 23%, with cheques, wire transfers and credit card payments making up 77%. Cash transaction limits for payment of services range between $2,000 and 15,000. The risk of TF is low in the insurance sector.

Use of cash in the IB sector and the IP sector is limited as payments for services are made primarily by way of wire transfer. In relation to Financing, use of cash is also limited as payment for services received is primarily via wire transfer or cheque. Where cash is accepted,

the maximum amount is $10,000 in accordance with the AMLTFCOP and represents only 13% of all payments for those entities. Cash is not accepted within the VASP sector given the virtual nature of the business. Financial transactions are executed primarily via wire transfer and VAs. Use of cash is also limited in the TCSP sector. The preferred method of payment for most entities is either cheque or wire transfer, with some entities also accepting credit/debit cards. Most licencees do not accept cash as payment for services but where cash is accepted, the maximum amount accepted may range from $1000 to $5000. Between 2020 and 2023, no entity accepted more than 10% of their total payment in the form of cash, with the average being approximately 3%.

Wire transfers and cheques are the main methods of payment for accountants, lawyers and notaries.

Limited cash and cheque payments are accepted. Wire transfers, cheques, cash and bank financing are the main payment methods accepted by the real estate sector; the use of cash is limited. Within the relevant legislation, namely the AMLRs, there is a 15,000 threshold which ensures that CDD measures are applied when conducting cash transactions in the DPMS sector and the HVGDs sector. Debit and credit cards, cheques and cash are the main payment methods accepted by the DPMS Sector. For the HVGDs wire transfer, cheques and bank financing are the main methods of payment used.

The overall vulnerability of cash being misused for the purposes of terrorism or TF in the VI is low.

3.6 Emerging Risks - Vulnerabilities

Additionally, emerging risks related to financial services business were considered such as new and emerging types of VASPs, Initial Coin Offering (ICO) and token issuance, stablecoins and off chain transactions.

A review of open-source material as well as cases under investigation by the RVIPF revealed an emerging risk for VASPs in terms of TF and TFS evasion, as those engaged in these activities take advantage of the lack of consistent regulation globally, ease of obscuring virtual transactions and rapidly evolving technology. Fundraising campaigns allegedly for charitable purposes, crowdfunding and social media campaigns accepting cryptocurrency have been

identified within the materials found[92]. These tend to be relatively small campaigns involving simpler methods and lower amounts of funds and is an appealing method of fundraising for terrorism financiers given the difficulties for investigators in distinguishing between genuine humanitarian causes in areas where there is known terrorist activity, and terrorist funding schemes. Recent prosecutions globally of donors have slightly inhibited this type of funding and led some groups to stop soliciting cryptocurrency donations, but it remains widespread.

VAs are known to be used by terrorist groups, in particular by ISIL in Asia and groups in Syria and terrorist groups that are using VAs often use stablecoins and experiment with anonymity enhancing cryptocurrencies. VAs have been identified by FATF as being particularly capable of undermining regulatory controls when they involve person-to-person transfers, with no regulated intermediary and no clear jurisdictional boundaries to the transaction[93]. The use of Stablecoins such as Tether (USDT) in particular, has been noted[94]. Self-hosted wallets and peer to peer transactions are emerging as an area where risks are not yet fully evaluated and therefore not sufficiently mitigated, making them vulnerable to misuse[95]. Non-Fungible tokens are not approached consistently across jurisdictions and have been found to be used in fraud and other financial crimes, as well as money laundering schemes, but less so with regard to proliferation or TF[96].

Perhaps the biggest threat from a TF perspective is the convergence of traditional fundraising methods with technology enabled fundraising. The use of multiple communication networks, social media platforms, cryptocurrencies, person to person transactions, and other virtual asset services in conjunction with traditional methods of movement through conventional financial systems means that the financial trail is more complex, convoluted and challenging to follow.

---

[93] FATF https://www.fatf-gafi.org/en/publications/Fatfrecommendations/targeted-update-virtual-assets-vasps-2024.html
[94] FATF https://www.fatf-gafi.org/en/publications/Methodsandtrends/crowdfunding-for-terrorism-financing.html US Department of Justice
https://www.justice.gov/opa/pr/cyber-scam-organisation-disrupted-through-seizure-nearly-9m-crypto
https://www.justice.gov/opa/pr/global-disruption-three-terror-finance-cyber-enabled-campaigns
[95] FATF https://www.fatf-gafi.org/en/publications/Fatfrecommendations/targeted-update-virtual-assets-vasps-2024.html US Department of the Treasury - 2024 National Terrorist Financing Risk Assessment
[96] Chainalysis https://go.chainalysis.com/crypto-crime-2024.html
US Department of the Treasury - 2024 National Terrorist Financing Risk Assessment
CFATF - Money Laundering & Terrorism Financing Risks Through the use of Virtual Assets and Virtual Asset Service Providers

This is likely to be appealing to terrorist organisations and those subject to sanctions looking to move funds illicitly and with access to multiple methods of doing so.

The evolution of the governance of LPLAs, for example using decentralised models of governance or organisation, poses challenges with identifying the persons in control of a legal person or arrangement. However, in the VI this cannot be done utilising a VI legal person.[97] To date, new governance models have primarily been used in the virtual asset industry and have been known by the name "decentralised autonomous organisation." The use of decentralised finance (DeFi) has been noted and presents issues in terms of identifying the controlling entity or person and the jurisdiction where they are operating, which makes DeFi arrangements appealing to those wishing to move funds for illicit purposes[98].

The European Union Terrorism Situation and Trend Report 2024 noted that Artificial Intelligence (AI) has also been embraced by some supporters of terrorism and violent extremism, who have integrated the use of generative AI and LLMs into their propaganda toolbox. Some right-wing actors are able to accelerate the spread of disinformation and hate speech online through the effective use of AI. Recent examples in the right-wing scene have involved AI-generated propaganda material and deepfakes containing racist or anti-Semitic messages or attempting to bypass an AI model's ethical safeguards and spread prohibited information through coded effects applied to seemingly irrelevant content. As deepfakes can alter videos in real time, there is a growing concern that livestreaming deepfakes could be used for terrorist purposes in the future to spread social alarm. AI has also been used to create fake identities and automated bots to manage chat groups.

Technology is also used to shield communications and activities from detection. In addition to periodic device formatting, freely accessible E2EE applications, VPNs, the dark web and cryptographic applications are commonly used to enhance the privacy of communications. With the development of immersive technology, training camps could be offered in realistic, (re-)created virtual environments and scenarios, as in the metaverse, which has already been used by young individuals in the jihadist milieu to simulate attacks. Investigations across

[97] As the legislation prohibits this although the vulnerability remains for group of legal persons / legal arrangements.
[98] Chainalysis https://go.chainalysis.com/crypto-crime-2024.html FATF https://www.fatf-gafi.org/en/publications/Fatfrecommendations/targeted-update-virtual-assets-vasps-2024.html

Member States show a stable use of cryptocurrencies as a means of transfer for TF. However, a shift away from the use of Bitcoin towards stablecoins was observed. [99]

As at the date of this report, geopolitical risks are rapidly changing and closer relationships between high-risk countries, for example North Korea, Iran and Russia, can forge new pathways for these countries to launder money, finance terrorism and proliferation and evade sanctions by establishing complex structures of LPLAs, including in countries that may not traditionally be seen as high-risk countries.

This matter will remain under review including by the CLEA policy of reviewing and disseminating quarterly TF risks and trends updates.

3.7 National Vulnerability

The National level vulnerability for TF was ML, based on a finding of ML for structural vulnerabilities, ML for the legal and regulatory framework and MH for the effectiveness of the framework primarily due to the impediments in the resourcing of law enforcement and the consequential limitations on the progression of matters relating to TF particularly as it relates to the misuse of legal persons and the transfer of VAs, which require particular skills, expertise and human and technical resources.

3.7.1 Structural Vulnerabilities

In relation to the structural elements, namely the rule of law, the national counter terrorism strategy, the national TF strategy and the engagement with counter parties on TF and terrorism, the overall vulnerability was rated as Medium-Low. The VI adheres to the rule of law with a democratically elected House of Assembly, a Governor who is responsible for law enforcement and matters of defence, and an independent and impartial judiciary. The National Counter Terrorism Strategy was implemented in 2022, and the National AML CFT Policy and Strategy were updated in in 2024. A national TF investigation and prosecution strategy was also being worked on by the authorities at the time of this report. Collaboration and cooperation with foreign counterparts in relation to financial crime generally and including TF specifically has increased since the MER with a marked increase in the use of outgoing requests by the FIA-AIU and other LEAs.

[99] European Union Terrorism Situation and Trend Report 2024 at page 10.

3.7.2 The Legal and Regulatory Framework as it Relates to Terrorist Financing – Compliance with International Standards

In relation to compliance with international standards regarding laws and regulations, as these relate to terrorism, TF, preventative measures, BO, cash couriers, the responsibilities and powers of law enforcement and investigative authorities as well as international cooperation the overall rating in terms of the vulnerability of the jurisdiction was ML.

As the VI had very recently undergone a Mutual Evaluation (published in 2024), this provided a useful starting point for an objective assessment of the level of compliance within the Territory. Additionally, consideration was given to the efforts made since the Mutual Evaluation to further enhance the legislative framework, as well as the vast amount of policy work undertaken.

Recommendation 5, which relates to the TF framework in the VI was rated Compliant, the WG was therefore satisfied that there were no significant issues to address in this regard. In relation to Recommendation 6 and the TFS requirements, all of these measures have either been addressed or in the final stages of being addressed, it is therefore concluded that this recommendation is satisfactorily addressed.

In relation to the misuse of LPLAs for TF, the requirements of recommendation 24 (transparency of legal persons) were reviewed by the WG as this is relevant as to whether adequate and accurate BO information can be obtained by law enforcement in relation to investigations into legal persons. Recommendation 24 was rated PC, however since that time a targeted RA of LPs and LAs has been concluded. The BVI Business and Limited Partnerships are now required to maintain the BO information, the Registered Agent must verify this similar to the agent's obligation under AMLTFCOP. Requirements on foreign companies' registered offices to include country of incorporation information have also been included. The Trustee Act has also been amended to ensure that there is a requirement to collect, keep and maintain adequate, accurate and up to date information on BO. Furthermore, requirements have been imposed relating to liquidators. Additionally in 2024 the VI was in the process of implementing a BO register to ensure all information on BO is maintained by a public authority and verified[100].

[100] This was implemented and came into effect on 2 January 2025.

Therefore, accurate and adequate information must now be held, and this strengthens the regime and further mitigates against the risk of abuse of companies for TF purposes.

Additionally, in order to review the VI's framework in relation to supervision of FIs and DNFBPs and how this may impact TF, as well as the powers of Law Enforcement and the international cooperation framework deficiencies in relation to Recommendations 10,11, 12, 17 and 15, 30, 31, 27 and 40 were considered as well as the VI's progress in addressing deficiencies and again it was concluded that no substantial deficiencies remain.

3.7.3 The Effectiveness of Measures to Prevent and Detect Terrorist Financing – Compliance with International Standards

In relation to the effectiveness of the jurisdiction in preventing and detecting TF, the evasion of TFS, the misuse of LPLAs, the sharing of information and international cooperation, as well as the use of financial intelligence. Again, the VI's MER provided a useful starting point in terms of an objective assessment of the level of effectiveness.

Additionally, the progress made since the conclusion of the Mutual Evaluation and improvements made to the CFT regime since that time have been considered, including in relation to resources, policies, training and the increased cooperation at the national level. The overall vulnerability score in relation to the effectiveness of the VI as it relates to combatting TF was MH.

Within the MER Immediate Outcome 9 (TF) was rated Moderate. Recommended Actions related to increasing training and the implementation of a national strategy relating to investigations and prosecutions. The ODPP has implemented a policy regarding prosecutions and the overall cross agency strategy is being finalised. A system has also been implemented to monitor TF risks and disseminate identified trends. Funding has also been granted for additional financial investigators at the RVIPF-FCU although these are not yet in place. Further enhancements are still in progress in relation to resources and the progression of investigations into prosecutions.

In relation to Immediate Outcome 10 recommendations related to improving oversight of implementation of TFS obligations by reporting entities and increasing risk understanding. The

FSC's approved 2024 Inspection schedule calls for the conduct of 50 compliance inspections based on inherent ML/TF/PF risks and supervisory concerns identified, 20 of which include a focus on TFS. Those twenty entities consist of TCSPs and IBs, as these sectors have been identified as posing a higher risk. The assessment includes a review of entities' TFS policies and procedures for ongoing monitoring, sanctions identification, screening, and reporting, and also considers sanctions training, and entities' overall testing of the efficacy of their sanctions framework. The inspections also assess the level of implementation and effectiveness of the entities TFS framework through sample testing of client files. Such sample testing aims to gauge the level of compliance as it relates to screening of BOs against relevant sanction lists (inclusive of appropriateness of screening and frequency) as well as the level of ongoing monitoring/ reporting (where applicable).

In addition to the onsite inspection programme, the FSC is conducting a desk-based review of 30 TCSPs, 10 of which are scheduled to have their sanctions procedures reviewed. These reviews will include a review of the effectiveness of the systems in place for such monitoring and the level of training provided to staff. Once complete, the results of these reviews will feed into supervisory risk models. The thematic review had been completed in Q4 2024 and at the time of the RA consideration was being given to remedial and enforcement actions.

Following the Russian invasion of Ukraine and the unprecedented growth of sanctions, the GO in response to the increased workload recruited an additional member of staff for a six-month period up until May 2023. The GO has undertaken Sanctions specific training between 2020 and 2023 including a 5 day training session on investigating financial crime including sanctions, maritime sanctions, proliferation financing, licencing and reporting to OFSI, processing sanctions applications, sanctions workshop including regulatory developments, risk typologies and corporate transparency issues, the Overseas Territories Sanctions Forum, sessions hosted by HMT and OFSI on sanctions, trusts, ownership and control, oligarchs, information sharing and the designations of individuals at the country level. In 2024 the sanctions function was delegated from the GO to the Sanctions Unit, led by the Sanctions Coordinator sitting in the AGC.

The Sanctions Unit is now comprised of the Sanctions Coordinator, a Policy Officer and a Data Specialist. A Licencing Specialist from the UK Foreign, Commonwealth and Development Office (FCDO) has been seconded to the Unit to assist in the functions of licencing primarily

and other functions as delegated. This specialist will serve until July 2025. It is intended that in the coming months the Unit will be staffed with a further policy officer and administration personnel. The FCDO, in supporting the capacity building of the VI in sanctions compliance, has facilitated the enrollment of 16 persons across various Government Agencies and Statutory Bodies on the ACAMS Certified Global Sanctions Specialist Course. The Sanctions Coordinator is currently enrolled, as well as personnel from FSC, FIA, British Virgin Islands Ports Authority, AGC, VI Shipping and Maritime Authority and HMC. It is envisaged that, on successful completion of the courses by these students, the VI's mandate as it pertains to sanctions implementation and enforcement will be better understood and executed. The Global Economic Sanctions C5 workshops and conference in November 2024 was attended by the Sanctions Coordinator and other personnel from the AGC and FIA and provided an opportunity for networking with other Jurisdictions on sanctions matters, trends and risks. Also in November 2024, FCDO, in collaboration with OFSI, delivered a one-day workshop. New staff are required to undertake courses where they do not already possess the relevant certificates.

The Sanctions Committee is a subcommittee of the CCA. After operating as an *ad hoc* committee since 2019, the Sanctions Committee was formally established on 26 June 2024 with specific terms of reference. Core members of the Sanctions Committee are the Sanctions Coordinator (as Chairman), the AGC, FIA, FSC and RVIPF (FCU). Associate membership extends to VI Shipping Registry, Department of Immigration, HMC, International Tax Authority, BVI Ports Authority, BVI Airports Authority, Ministry of Finance, Civil Aviation Authority and ODPP. There is also provision in the Terms of Reference for ex-officio members to attend meetings as needs be. The Sanctions Committee meets monthly.

The Sanctions Committee provides an avenue for collaboration and cooperation, where sanction matters that require high level cooperation and coordination can be discussed, including reporting and updating on suspected sanctions breaches, discussing typologies and assessing risks, discussing media and other inquiries, as well as discussions on drafting and amendment of policy and procedural documents can take place. This will allow for greater efficiency and effectiveness in sanctions implementation, through shared understanding and input in the process by key agencies and/or departments.

In relation to IO5 and the transparency of LPLAs, much work has been done on understanding risks and raising awareness of the risk of misuse of VI legal persons to facilitate ML and TF in the VI and abroad.

Further enhancements are still in progress in relation to resources and the progression of investigations into prosecutions.

3.8 Overall Vulnerability Rating of Each Sector – Adjusting for National Vulnerability and Materiality.

In relation to the overall vulnerability of the VI to TF, the WG considered the vulnerability of each sector and considered the findings regarding vulnerability at the national level as well as materiality and considered whether any adjustment was required.

It is recognised that materiality plays a role in relation to inherent risk. Therefore, regulated sectors were ranked according to their materiality based on the number of entities in the sector, sectoral risk, assets under management or turnover, number of employees etc. Other areas reviewed above (legal persons, cash and NPOs) were also placed according to their materiality rating. Then any adjustments to the inherent risk rating based on materiality was considered. Those with lower materiality had their vulnerability scores reduced.

Table 22 - Sector and Area Materiality

Ranking	Sector	Size	Key features of materiality
1	TCSP[101]	287 (includes 105 CSPs and 133 TSPs)	Trusts Under Administration - $171.10 billion[102]
2	Legal Persons	350,000	NA

[101] Note this combines both the CSP sector and the TSP sector.
[102] This does not relate to CSPs.

3	VASPs	42 (plus 10 non-operating pending registration)	65 applicants for registration, 9 of which have been registered under the VASPA thus far. Nine applicants (all startups that had not yet launched) withdrew their applications and four applications were refused. Of the 43 applications pending decision, 33 are established entities subject to the transitional provisions and are currently undertaking business and 10 are new applicants which have not commenced business. [103] The FSC understands and expects that numbers in relation to customers serviced and transaction sizes will be high
4	Investment Business	230	NAV - $9.02 billion
5	Banking	7	Assets Held - $3.27 billion
6	Lawyers	36	$33,26 billion (value of transactions for relevant business)
7	Domestic Insurers	38	Value of Premiums - $107.10 million
	Captive Insurers	45	Gross assets held - $1.39 billion
	Managers	6	Management fees - $0.95 million
	Intermediaries	14	Commissions - $22.19 million
8	MSBs	2	Total transaction value - $53.64 million
9	Financing	2	Avg. value of transactions - $$5,828

[103] At the time of the risk assessment, it was anticipated that all applicants would be decided upon by the end of Q1 2025.

10	Insolvency	28	(Unknown)
11	Accountants (conducting relevant financial business)	6	$287,277,673 million (value of transactions for relevant business)
12	Real Estate Agents	13	$59.42 million (value of transactions for relevant business)
13	Use of cash	N/A	Unknown
14	HVGDs	13	$31.67 million (value of transactions for relevant business)
15	DPMS	5	$1.6 million (value of transactions for relevant business)
16	NPOs	117	$38 million (value of transactions)

Table 23 - Overall Vulnerability Rating for Each Sector and Area Adjusted for National Vulnerability and Materiality

	Sector Vulnerability rating	**Vulnerability after adjustment for national vulnerability findings and materiality**	**Identified Typologies**
Banking	L	L	2
MSB	ML	ML	2
Insurance	L	L	3
Investment business	ML	ML	3
Financing	L	L	3
VASPs (and VAs)	MH	MH	1, 2
TCSPs	MH	MH	1, 3
Insolvency	L	L	3
Lawyers/ Notaries	ML	ML	3
Accountants	ML	L	3

DPMS	ML	ML	3, 4
Real Estate Agents	L	L	3
High Value Goods Dealers	ML	L	3
Legal Persons and Arrangements	MH	MH	1
NPOs	L	L	1
Cash	L	L	4

Table 24 - The Overall Vulnerability Rating for Each Typology:

Typology 1: VI legal entities are abused for TF purposes.	MH
Typology 2: VI entities used as a transit for funds that are intended to be used for terrorism purposes abroad, with funds being sent via the VI such as a bank (L), MSB (ML) or VASP (MH).	MH
Typology 3: The VI service providers (FIs or DNFBPs) knowingly or unknowingly facilitate the movement of funds for terrorism purposes but without the funds actually entering or moving through the jurisdiction – for example, VI lawyers providing services to clients that support foreign terrorism.	ML
Typology 4: The VI facilitates the movement through or from the VI of cash, BNIs or PMS (or dual use goods as relevant to TF).	L

4. Likelihood: Threat Multiplied by Vulnerability

To assess likelihood, the threat rating for each typology was multiplied by the highest vulnerability score of any of the sectors relevant to that typology. This was done using the table below:

Table 25 - Likelihood Calculation Table:

Threats	**Vulnerabilities:**	L	ML	MH	H
L		L	ML	ML	MH
ML		ML	ML	MH	MH
MH		ML	ML	MH	H
H		MH	MH	H	H

Table 26 - Typology Likelihood Ratings

	Threat	Vulnerability	Likelihood
Typology 1	MH	MH	MH
Typology 2	MH	MH	MH
Typology 3	ML	ML	ML
Typology 4	L	L	L

5. Controls

5.1 Private Sector Controls

To consider the effect that identified controls had on the level of risk, first the private sectors' implementation of controls was considered. Whilst these were considered to some extent in relation to the vulnerability caused by a high-level lack of controls at the national level, at the sectoral levels this involved consideration of the implementation of CDD and EDD measures including for BO (holding accurate and up-to-date information) by the private sector and the impact this had on mitigating the risk of TF. The extent to which entities were carrying out entity-level TFRAs and implementing corresponding, targeted controls was considered as well

as the quality of the suspicious transaction reports filed. The level of compliance with TFS was also a factor. Employee training and knowledge relating to TF and TF risk were also considered. The level of compliance with these requirements was rated using results of onsite and offsite visits as well as the expertise of the supervisors and questionnaires sent out to industry.

The Scoring table used for the rating of the compliance of entities was:

- Good - Over 85% of entities fully compliant with requirement
- Satisfactory - Between 70% and 85% fully compliant
- Weak - Between 51% and 9 % fully compliant
- Very weak - 50% or below compliance levels

The results of the findings were analysed, and the weighting of the various factors was adjusted depending on their pertinence to the sector. This led to an overall control score for each sector of Good, Satisfactory, Weak or Very Weak.

5.1.1 Banking

FSC's findings reveal a high level of compliance with CDD and EDD within the banking sector. Feedback received from other competent authorities such as ITA, AGC and RVIPF who request information from banks indicates that information has been provided in a timely manner. These authorities are more likely to request specific account information. FSC has not requested any such information during the period, However, due to a recent IC request, FSC recently sought banking information on behalf of a foreign regulator for VI entities believed to be holding bank accounts in the Territory. The information requested, which consisted of account opening applications which included details of BO, bank statements and transaction listings and company extracts, was provided by the bank within the timeframe stipulated for responding. This allowed the FSC to respond to the foreign regulator who provided feedback indicating that the information provided was useful to their investigation. Given the nature of the activities supervised by the FSC, this is consistent with what FSC expects.

All banks licenced in the VI have conducted an institutional RA, which included an assessment of their TF risk. These entities have considered their potential exposure to TF based on

information provided from open-source material and existing national TFRAs when designing their internal controls policies and procedures. In addition, most banks have completed a full TFRA with the remaining in the process of doing so.

The FSC's review of SAR processes in banks found such practices satisfactory and commensurate with risk. Between 2020 to 2023, banks in the VI filed a total of 636 SARs, or roughly 5% of all SARs filed during that time. This sector ranks third for the number of SARs filed. Given the quality of information submitted, the high average of filing entities, and the relatively large number of SARs submitted, the overall quality is good.

Based on a review of the compliance officer reports that must be submitted to the FSC on an annual basis as well as onsite inspections, relevant employees of all banking licensees have received TF training, including training on the identification of TF within the last 3 years. Due to the systemic importance to the Territory's economy, all banks are monitored by the FSC's SSU. Ongoing desk-based reviews by the SSU have found that risk mitigation policies and procedures that have been updated within the reporting period are in place in all entities and relevant controls have been implemented. In most banking institutions, all relevant staff are fully aware of TF risk and the TF risk to which the Territory is exposed and understand how it impacts the work of the organisation as evidenced from training information provided through compliance officer reports and other returns that have been reviewed by the supervisor.

Targeted Financial Sanctions Compliance –Inspection Results, Compliance with Requirements and Breaches:

Two of the seven banks (29%) have been inspected within the past two years. All inspections for banks are full scope and encompass a TFS review and assessment. The licencee inspected in 2023 received a rating of Largely Compliant and the findings noted that the bank had established sanctions policies and procedures that were largely appropriate to ensure compliance with TFS obligations. Furthermore, the assessment revealed the licencees' implementation of appropriate screening and monitoring procedures for all customers and transactions. Through inquiry and sample testing, it was noted that there were no instances where a client during take-on or during the business relationship had any sanction exposure. The findings also indicated continuous measures to mitigate TFS risk through the Bank's continuous sanctions training of staff, and continuous testing of its TFS procedures and systems. It is expected that all seven (7) banks will be inspected by the end of 2025.

Table 27 – Banking Sector Controls

CDD and EDD measures implemented	Entities carry out entity-level TFRA and implement corresponding controls.	Quality of Reporting of Suspicious Transactions	Employee training	Knowledge of TF and understanding of TF risk by the sector	Risk mitigation policies and procedures	TFS compliance	**Overall control score**
Good	Good	Good	Good	Good	Good	Good	Good

5.1.2 Money Service Businesses

FSC's findings reveal a high level of compliance with CDD and EDD measures, which take into consideration BO information and ensure reliance on original documentation to verify individuals and key CDD information. Such controls also require BO information to be up-to-date and valid. Two previous MSB inspections reveal a rating of largely compliant as it relates to CDD and verification. Shortcomings were identified with the application of EDD measures within one MSB, which received a rating of Partially Compliant for EDD. The other MSB inspection revealed only minor shortcomings relating to EDD, and a rating of Largely Compliant was assigned.

100% of entities have carried out a TFRA during the reporting period and implemented all relevant controls in line with the findings of their TFRA.

Based on a review of the compliance officer reports that must be submitted to the FSC on an annual basis, employees within the MSB sector have been trained in TF and the identification of TF within the last 3 years. Further entities have risk mitigation policies and procedures, updated within the data period, that specifically address TF risk.

In 2022, one MSB underwent an onsite inspection which included a review of its TFS procedures. The findings of that inspection indicate that the licencee has established TFS procedures relating to screening, ongoing monitoring and reporting. The inspection did not identify any shortcomings with the MSB's TFS framework. Furthermore, there were no

deficiencies arising from the sample testing of client files, which evidenced the incorporation of sanctions exposure within the client RA, and ongoing screening and monitoring of customers and transactions.

Relevant staff of MSBs are fully aware of TF risk and the TF risk to which the Territory is exposed and understand how it impacts the work of their organisation as evidenced from training information provided through compliance officer reports and other returns that have been reviewed by the supervisor.

During the reporting period only 2 SARs were filed by MSBs, which accounts for 0.02% of the total number of SARs filed during this period. Neither SAR was TF-related. The number of SARs filed appears low given the cash-intensive nature of the sector, however, the quality of information submitted is good.

Table 28 – Money Service Businesses Sector Controls

CDD and EDD measures implemented	Entities carry out entity-level TFRA and implement corresponding controls.	Quality of Reporting of Suspicious Transactions	Employee training	Knowledge of TF and understanding of TF risk by the sector	Risk mitigation policies and procedures	TFS compliance	**Overall control score**
Good	**Good**	**Good**	**Good**	**Good**	**Good**	**Good**	**Good**

5.1.3 Insurance

The desk-based reviews raised no issues surrounding the implementation of CDD/EDD within the insurance sector. 88% of entities have carried out a TFRA during the data period while 12% are currently working on completing a TFRA. 75% have implemented relevant controls in line with the findings of their TFRA, while 12.5% have implemented some controls based on the findings of their TFRA and another 12.5% have not implemented any controls based on any TFRA.

Employees across the insurance sector have been trained in TF and the identification of TF within the last 3 years. 75% of licencees have risk mitigation policies and procedures, updated within the data period, that specifically address TF risk while 12.5% have risk mitigation

policies and procedures, updated during the data period that refer to and address TF risk to some extent. The remaining 12.5% do not have any risk mitigation policies and procedures that refer to and address TF risk.

Given the identified low level of risk within the insurance sector, no inspections focused on TFS have been carried out within the insurance sector during the reporting period to ascertain the sector's level of compliance with its sanctions obligations. However, 52 licencees have been subject to desk-based reviews between 2022 and 2023.

Relevant staff within 87% of licencees are fully aware of TF risk and the TF risk to which the Territory is exposed and understand how it impacts the work of their organisation. In the remaining 13% most relevant staff are fully aware of TF Risk and the TF risk to which the Territory is exposed and understand how it impacts the work of their organisation.

A total of 25 SARs were submitted during the review period, accounting for 3% of all SARs submitted. None of these were TF-related, given the low-risk nature of the insurance products offered by this sector, the level of filings is considered commensurate with overall sector risk. The quality of information submitted, however, is generally not considered to fully cover the threshold for a SAR, as a number of the SARs received were later categorised as UARs (unusual activity reports) by the FIA or not analysed rated as low because the information contained did not adequately describe a suspicion. Therefore, the resulting assessment aligned more with a satisfactory quality having regard to good quality in more than half of the SARs filed by this sector.

Table 29 – Insurance Sector Controls

CDD and EDD measures implemented	Entities carry out entity-level TFRA and implement corresponding controls.	Quality of Reporting Suspicious Transactions	Employee training	Knowledge of TF and understanding of TF risk by the sector	Risk mitigation policies and procedures	TFS compliance	**Overall control score**
Good	**Satisfactory**	**Satisfactory**	**Good**	**Good**	**Good**	**Satisfactory**	**Good**

5.1.4 Investment Business

Based on findings of inspections conducted between 2020 and 2022, the IB Sector has generally established CDD controls, requiring risk based CDD and verification of BOs (via the collection of accurate and up-to-date information). Inspection findings demonstrate a high level of implementation with CDD procedures, with 8 of the 11 IB licencees inspected (for CDD) receiving a rating of Largely Compliant or Compliant. There was, however, a decrease as it relates to the level of EDD conducted with 6 of the 11 licencees inspected demonstrating shortcomings in the implementation of EDD measures and receiving a rating of partially or non-compliant. For those licencees where deficiencies were identified, corrective actions were imposed which required full remediation. Such remediation requires the licencees to amend established controls and review their portfolios to ensure appropriate measures are applied. The corrective actions also require continuous reporting to the supervisory division until an appropriate level of effective compliance is attained.

According to the annual AML Returns, 97 IBs have conducted an institutional RA, which included an assessment of their TF risk. Based on this analysis and assessment, the FSC has determined that IBs should be reviewed to understand and address this risk. Therefore, thematic reviews assessing the conduct of institutional RAs (for ML and TF) and whether the sector understands its ML and TF risk have been included in the 2024 Inspection programme and will commence in the 4th quarter of 2024, through quarter 1 of 2025. While this assessment is still underway, the initial findings illustrate the conduct of Institutional RAs for 75% of the IB Licencees inspected. A review of the institutional RAs largely evidenced the consideration of both ML and TF risks.

With respect to Asset and Investment Managers, 50% have carried out a TFRA during the data period, however, 25% have not. 12.5% have considered TF risk, but have not completed a full TFRA, while another 12.5% are currently working on a TFRA. 75% of licencees have implemented relevant controls in line with the findings of the TFRA and 25% have implemented some controls based on the findings of their TFRA. 50% of Asset Administrator licencees have carried out a TFRA during the data period and have implemented all relevant controls in line with the findings of their TFRA, while the other 50% are currently working on a TFRA.

60% of Brokers/Dealers have carried out a TFRA during the data period, while 20% have considered TF risk, but have not completed a full TFRA, and another 20% are currently working on a TFRA. 80% have implemented relevant controls in line with the findings of their TFRA or consideration of their TF risk while 20% have implemented some TF controls independent of a TFRA. The one licencee holding an exchange licence has carried out a TFRA during the data period and has implemented relevant controls in line with the findings of its TFRA.

All relevant employees in 87.5% of the Asset and Investment Manager entities have been trained on TF and the identification of TF within the last 3 years, while 12.5% of licencees have had most of their employees trained on TF and the identification of TF within the last 3 years. In relation to Asset Administrators, all relevant employees across the sector have been trained in TF and the identification of TF within the last 3 years, as have all relevant employees across the Broker/Dealer sector and Exchange sector.

62.5% of Asset and Investment Manager licencees have risk mitigation policies and procedures, updated within the data period, that specifically address TF risk. The remaining 37.5% have risk mitigation policies and procedures, updated during the data period that refer to and address TF risk to some extent. 50% of Asset Administrator licencees have risk mitigation policies and procedures, updated within the data period, that specifically address TF risk, while 50%have risk mitigation policies and procedures, updated during the data period that refer to and address TF risk to some extent.

In relation to Broker/Dealers 40% of the licencees have risk mitigation policies and procedures, updated within the data period, that specifically address TF risk, while 60% have risk mitigation policies and procedures, updated during the data period that refer to and address TF risk to some extent. The Exchange licencee has risk mitigation policies and procedures, updated within the data period, that specifically address TF risk.

In relation to Asset and Investment Managers**, i**n 87.5% of licencees, all relevant staff are fully aware of TF risk and the TF risk to which the Territory is exposed and understand how it impacts the work of their organisations. In 12.5% of licencees most relevant staff are fully aware of TF Risk and the TF risk to which the Territory is exposed and understand how it impacts the work of their organisation. For Asset Administrators, all relevant staff are fully

aware of TF risk and the TF risk to which the Territory is exposed and understand how it impacts the work of their organisations. As regards brokers/dealers, all relevant staff in 60% of licencees are fully aware of TF risk and the TF risk to which the Territory is exposed and understand how it impacts the work of their organisations, while most relevant staff in 20% of licencees are fully aware of TF Risk and the TF risk to which the Territory is exposed and understand how it impacts the work of their organisation. Finally, in relation to exchanges all relevant staff within the licencee are fully aware of TF risk and the TF risk to which the Territory is exposed and understand how it impacts the work of their organisations.

Between 2020 and 2023, 115 SARs were received, which accounts for only 0.93% of total SARs filed, none of which were TF-related. Given the size of the IB sector, both the number of entities filing SARs and the number of SARs filed during the reporting period appears low.

With respect to quality, most SARs received from this sector were considered to be poor and subsequently reclassified as UARs or low-priority by the FIA, because the information received did not meet the threshold to constitute a SAR.

Table 30 – Investment Business Sector Controls

CDD and EDD measures implemented	Entities carry out entity-level TFRA and implement corresponding controls.	Quality of Reporting of Suspicious Transactions	Employee training	Knowledge of TF and understanding of TF risk by the sector	Risk mitigation policies and procedures	TFS compliance	**Overall control score**
Satisfactory	**Satisfactory**	**Weak**	**Good**	**Good**	**Good**	**Good**	**Satisfactory**

5.1.5 Financing

Regarding the implementation of CDD/EDD measures, no issues have been identified including in the collection of BO information. The clientele in this sector is very localised and limited to small transactions. 50% of entities have carried out a TFRA during the reporting period and implemented all relevant controls in line with the findings of their TFRA. 50% of entities have not carried out a TFRA and have therefore not implemented any controls specifically based on any TFRA.

Employees across the sector have been trained in TF and the identification of TF within the last 3 years. All entities have risk mitigation policies and procedures in place, updated within the data period, that specifically address TF risk (although not based on the results of a specific TFRA). Relevant staff are fully aware of TF risk and the TF risk to which the Territory is exposed and understand how it impacts the work of their organisation.

During the reporting period only 2 SARs were filed by MSBs, none of which were TF-related. This accounts for 0.02% of all SARs received by the FIA during that time. The overall quality of the SARs received, however, was good.

Table 31 – Financing Sector Controls

CDD and EDD measures implemented	Entities carry out entity-level TFRA and implement corresponding controls.	Quality of Reporting of Suspicious Transactions	Employee training	Knowledge of TF and understanding of TF risk by the sector	Risk mitigation policies and procedures	TFS compliance	**Overall control score**
Good	**Satisfactory**	**Good**	**Good**	**Good**	**Good**	**Good**	**Good**

5.1.6 Virtual Asset Service Providers

As part of the application process, the FSC has reviewed the technological systems including AML/CFT obligations via live demonstrations. Firms who offer solely to institutional clients have been more readily able to demonstrate compliance with the AML/CFT regime. The FSC reviews the VASPs' policies and procedures to ensure they include effective mechanisms for collecting, verifying, and securely transmitting required information about both the sender and recipient of virtual asset transfers. The FSC also assesses the functionality of VASPs' transaction monitoring systems to ensure they can detect and flag non-compliant transactions.

In relation to established VASPs, 22 were compliant or largely compliant with AML / CFT requirements, 19 were partially compliant and 4 were non-compliant. In relation to startups, 5 were compliant or largely compliant, 3 were partly compliant and 2 were non-compliant. Deficiencies identified include sanctions screenings, adequate KYC procedures and failure to implement travel rule requirements (as required).

In large part the VASP applicants have been able to demonstrate that they have AML/CFT procedures[104] and controls in place. Where procedures were not in place for a minute number of applicants at the onset of submissions, they have since been able to demonstrate that they have adapted the necessary AML/CTF policies and controls.

A summary of these concerns has also been presented to the industry during various outreach activities, with the goal of assisting future applicants in submitting complete and comprehensive applications and providing clarifying information regarding regulatory requirements and expectations. Some of the issues identified include adequacy of AML/CFT policies and procedures that are not bespoke to VI legislative and regulatory requirements to ensure adequate sanction screening mechanisms at the onboarding phase and on a continuous basis.

The FSC has conducted a gap analysis on each applicant and where deficiencies have been identified applicants have been engaged to make corrective action prior to consideration of approval. Outsourcing Risk was also an identified area of concern whereby VASP applicants outsource certain AML/CFT functions to group-related parties and/or non-group-related parties. This primarily relates to client onboarding, continuous monitoring and sanction screening. Identified deficiencies in applicants' policies around outsourcing include no procedures for assurance testing, lack of continuity of function (where for example the outsourcing arrangement came to an immediate halt) and no clear effective system to ensure sufficient oversight of the outsourced activities as required by VI legislation. Lack of service level agreements was also an issue, primarily where group entities were contracted. Compliance with the application of the Travel Rule Compliance was also a concern as in some instances, applicants were unable to demonstrate that they have addressed measures and procedures which must be undertaken, where that VASP or intermediary service provider may be located in countries that do not have commensurate travel rules requirements. The FSC has

[104] Applicants are required to demonstrate their ability to comply with the VI's AML/CFT framework since December 2022. The scope of the requirements includes the ability to demonstrate that they have established and maintain procedures that screen and verify the identity of clients. The applicants are also required to prove their policies and procedures are effective. Applicants must demonstrate that they have adopted a risk-based approach to identifying risk and for the monitoring of financial activity, including compliance with sanction orders. Additionally, applicants must be able to demonstrate that they have appropriate policies to comply with the travel rule. This includes providing evidence that said compliance has been in effect since December 2022. As a measure of this, all applicants are subjected to a VASP pre-authorisation questionnaire. The assessment is specific to each applicants' activities and resulting risk and helps to inform its AML risk assessment.

also noted that some policies are broad and do not prescribe specific compliance requirements such as the collection of wallet addresses for each relevant transaction.

In relation to entities carrying out entity-level TFRA and implementing corresponding, targeted controls:
24% of entities are currently working on a TFRA, while 68% have carried out a TFRA during the data period, and 8% have considered TF risk but have not completed a full TFRA. 62% of entities have implemented all relevant controls in line with the findings of their TFRA. 12% have implemented some controls based on the findings of our TFRA and 18% have implemented some TF controls independent of a TFRA. 8% of entities have not implemented any controls based on any TFRA.

79% of entities have risk mitigation policies and procedures, updated within the data period, that specifically address TF risk. 12% have risk mitigation policies and procedures, updated during the data period that refer to and address TF risk to some extent, while 6% have risk mitigation policies and procedures that cover TF to some extent but have not been updated during the data period.[105]

As part of the application process, some VASP applicants outsource certain AML/CFT functions to group-related parties and/or non-group related parties. This primarily relates to client onboarding, continuous monitoring, and sanction screening. Identified deficiencies in applicants' policies around outsourcing include no procedures for assurance testing, lack of continuity of function (where for example the outsourcing arrangement came to an immediate halt) and no clear effective system to ensure sufficient oversight of the outsourced activities as required by VI legislation. Lack of service level agreements also was an issue primarily where group entities were contracted.

In 79% of entities all employees have been trained on TF and the identification of TF within the last 3 years. In 15% of the entities, it is most employees who have been so trained. In 6% of the entities, most employees have not been trained in TF and the identification of TF within the last 3 years.[106]

[105] Responses based on TF Risk Assessment survey to entities
[106] Responses based on TF Risk Assessment survey to entities

In 85% of entities all relevant staff are fully aware of TF risk and the TF risk to which the Territory is exposed and understand how it impacts the work of their organisation. In 12% of entities most relevant staff are fully aware of TF Risk and the TF risk to which the Territory is exposed and understand how it impacts the work of their organisation. In 3% of entities, however, only some staff are aware of TF risk and the TF risk to which the Territory is exposed and understand how it impacts their organisation and sector.[107]

87.5% of all SARs received by the FIA during the reporting period were filed by VASPs. Eighty-eight of these SARs were TF-related. However, the majority of SARs received by this sector were submitted by one BVIBC acting as a VASP. The quality of SARs received from one VASP that is responsible for a large number of SARs filed has been found lacking due to inaccurate reporting, transaction date discrepancies, misleading narration, and lack of suspicion explanation and transparency. However, the quality of the information submitted by most VASPs is satisfactory. As such, the overall quality of SARs within this sector is considered satisfactory.

Table 32 – Virtual Asset Service Providers Sector Controls

CDD and EDD measures implemented	Entities carry out entity-level TFRA and implement corresponding controls.	Quality of Reporting of Suspicious Transactions	Employee training	Knowledge of TF and understanding of TF risk by the sector	Risk mitigation policies and procedures	TFS compliance	**Overall control score**
Satisfactory	Satisfactory	Satisfactory	Satisfactory	Satisfactory	Satisfactory	Satisfactory	**Satisfactory**

5.1.7 Trust and Corporate Service Providers

[107] Responses based on TF Risk Assessment survey to entities

Implementation of CDD and internal controls across the sector is satisfactory but require improvement. Findings from onsite inspections show a need for implementation of corrective measures concerning CDD/EDD though entities generally have controls in place.

Both desk-based and onsite reviews show a high level of compliance with the ability to identify BO. Some issues surrounding full CDD and verification have been identified, which include the ability to understand the nature of business and circumstances of clients and identification of the BO where a complex or layered structure is presented. However, when responding to international cooperation requests the FSC has been able to provide BO information when requested and no counterpart has identified that such information is not accurate.

The requirement under the AMLTFCOP to conduct institutional RAs came into force in the latter part of 2022. Licencees were, therefore, required to undergo their own self-assessment in 2023. Consequently, the FSC's review of entities' institutional RAs commenced in 2024. As of November 2024, eight entities have been inspected in relation to Institutional RA. Based on survey results, however, 15% of licencees in this sector are currently working on a TFRA. 56% have carried out a TFRA during the data period and 29% have considered TF risk but have not completed a full TFRA. 60% of licenced TCSPs also indicated that they have implemented relevant controls in line with the findings of their TFRA, while 20% have implemented some controls based on the findings of their TFRA. Another 20% have implemented some TF controls independent of a TFRA.

In 79% of licencees, all employees have been trained on TF and the identification of TF within the last 3 years, while 21% have trained most of their employees on TF and the identification of TF within the last 3 years.

70% of TCSPs have risk mitigation policies and procedures, updated within the data period, that specifically address TF risk. 23% have risk mitigation policies and procedures, updated during the data period that refer to and address TF risk to some extent and 7% have risk mitigation policies and procedures that cover TF to some extent but have not been updated during the data period.

During the reporting period, TCSPs submitted a total of 1,313 SARs. This represents 10.61% of all SARs received by the FIA during that period. Only 2 of these were TF-related. The larger

TCSPs submitted the majority of the SARs. The quality of information submitted in the SARs filed by TCSPs is generally acceptable. However, some SARs lack a reason for suspicion, a clear nexus to the VI, or details of the reported subject. At times, SARs received by these entities are more reactive rather than proactive.

Overall, the quality of SAR reporting with the TCSP sector is considered satisfactory. However, given the size of the sector and the number of SARs filed, based on the number of clients held by each TCSP and other risk factors, the level of reporting is not commensurate with the inherent risk of this sector.

Targeted Financial Sanctions Compliance –Inspection Results, Compliance with Requirements and Breaches:

Twenty TFS themed inspections were conducted during 2020 – 2023, which focused on the entities' ability to identify TFS exposure, and the adequacy of their monitoring and reporting procedures. In relation to staff awareness, within 80% of entities all relevant staff were fully aware of TF risk and the TF risk to which the Territory is exposed and understand how it impacts the work of their organisation. In 18% of TCSPs most relevant staff were fully aware, while in 2% of entities only some staff were aware of TF risk and the TF risk to which the Territory is exposed and understand how it impacts their organisation and sector.

Table 33 – Trust and Corporate Service Providers Sector Controls

CDD and EDD measures implemented	Entities carry out entity-level TFRA and implement corresponding controls.	Quality of Reporting of Suspicious Transactions	Employee training	Knowledge of TF and understanding of TF risk by the sector	Risk mitigation policies and procedures	TFS compliance	**Overall control score**
Satisfactory	**Satisfactory**	**Satisfactory**	**Satisfactory**	**Satisfactory**	**Satisfactory**	**Satisfactory**	**Satisfactory**

5.1.8 Insolvency

Given the low level of TF risk within the IP sector, there have been no inspections conducted within the reporting period. However, all IPs are required to establish and maintain appropriate

CDD and EDD measures, in line with the AMLTFCOP. All entities indicated that they have carried out a TFRA during the data period and have implemented all relevant controls in line with the findings of their TFRA. Employees across the sector have been trained in TF and the identification of TF within the last 3 years. All entities have risk mitigation policies and procedures, updated within the data period, that specifically address TF risk. There were no instances where enforcement action needed to be taken against any licencee within the insolvency sector during the reporting period

Relevant staff within the licencees are fully aware of TF risk and the TF risk to which the Territory is exposed and understand how it impacts the work of our organisation.

During the reporting period 36 SARs were filed by IPs, which represents 0.29% of all SARs received. However, none of these SARs were TF-related. The quality of reporting is good and given the small size of the sector, this level of reporting is appropriate

Table 34 – Insolvency Sector Controls

CDD and EDD measures implemented	Entities carry out entity-level TFRA and implement corresponding controls.	Quality of Reporting of Suspicious Transactions	Employee training	Knowledge of TF and understanding of TF risk by the sector	Risk mitigation policies and procedures	TFS compliance	Overall control score
Good	**Good**	**Good**	**Good**	**Good**	**Good**	**Good**	**Good**

5.1.9 Accountants

7 of the 18 registered accountants conduct relevant business under the realm of IPs and have implemented CDD obligations/ internal controls across the sector or with AML/CFT compliance and awareness within the sector (according to FSC). 5 out of the 18 registered accountant engage in accounting activities such as auditing and not relevant financial business. Based on an initial desk-based review, while the remaining 6 registered accountants have AML/CFT policies in place that appeared to be in line with what is required in the AML/CFT legislation, these policies appeared to be generic and not risk based. Furthermore, some of the accountants do not have clear policies as it related to conducting CDD, specifically to identify the BOs, and they did not have any specific policies or procedures for holding adequate,

accurate and up to date information. As it relates to TF procedures, 66% of the accountants have specific targeted financial sanction procedures such as screening and reporting. While no TFS specific inspections have been conducted over the prior two years, the 2024 onsite inspection had an area of focus as it relates to financial sanctions obligations.

Most accountants possess a general understanding of their TF risk as evident by their policies, procedures, systems and controls within their compliance programme as it relate to reporting and screening in keeping with their TFS obligations under the VI financial Sanction Guidelines 2023.

The recordkeeping measures are adequate as all accountants have indicated that they have record-keeping procedures and that they maintain records for 5 years and over in some cases. As it pertains to ongoing monitoring, most of the accountants did not provide sufficient policies and procedures to show that they conduct ongoing monitoring of their clients. Most accountants indicated that they do not place reliance on third parties and conduct and collect their own CDD. In relation to measures for PEPs, while many of the accountants do have policies, processes, and procedures in relation to PEPs and are aware of their obligation to identify and verify PEPs as well as apply the relevant ECDD measures, the process and procedures implemented to screen and monitor are not ongoing. As it relates to the quality of Reporting of Suspicious Transactions, between the period 2021-2023, 10 SARs were filed by 3 entities and it was indicated by the FIA-AIU that the quality of the SARs filed by the entities in this industry contained relevant information and provided valuable intelligence.

Between September 2024 – October 2024, FIA-SEU conducted and concluded an onsite inspection on two accounting firms for the period 2021 – 2023. Each accountant received an overall rating of partially compliant due to deficiencies within their AML/CFT policies, procedures, systems and controls which coincides with the findings of the initial desk-based review highlighted above. Some deficiencies included inadequate institutional and customer risk assessment, generic compliance programmes which were not risk-based, inadequate CDD and ECDD measures, lack of an independent audit and poor implementation of their financial sanctions obligations as while the entities did have sufficient policies and procedures in relation to financial sanctions, they could not adequately demonstrate that screenings were being conducted systematically, at the start of the business relationship and on an ongoing basis. While the entities have a general understanding and knowledge of their AML/CFT obligations

there is some room for improvement. Therefore, in addition to remedial actions, the assessed entities were issued guidance documents in relation to institutional risk assessment, transaction monitoring, beneficial ownership and enhanced customer due diligence to provide further guidance to improve their AML/CFT/CPF measures and mitigate the risk of ML/TF and PF within their sector.

Although the trainings conducted covered the broad AML/CFT/CPF obligations, there were deficiencies: The trainings were not risk-based, targeted, or tailored to the appropriate employee responsibility in keeping with the requirements of AMLTF Code. Some of the training was not designed to test employee's knowledge of money laundering, terrorist financing and proliferation financing issues commensurate with established standards pursuant to section 48 of the AMLTF Code. And therefore, the entities were not able to adequately demonstrate that that employee had a good understanding of their AML/CFT/CPF obligations.

Table 35 – Accounting Sector Controls

CDD and EDD measures implemented	Entities carry out entity-level TFRA and implement corresponding controls.	Quality of Reporting of Suspicious Transactions	Employee training	Knowledge of TF and understanding of TF risk by the sector	Risk mitigation policies and procedures	TFS compliance	Overall control score
Weak	**Weak**	**Good**	**Satisfactory**	**Weak**	**Satisfactory**	**Satisfactory**	**Satisfactory**

5.1.10 Lawyers and Notaries

Based on an initial desk-based review, over 80% of the registered legal practitioners have undertaken an institutional RA but most have not considered specific TF risk, except most of the larger global firms who are more susceptible to these risk based on their clientele. The legal practitioner sector does have general policies and procedures in place which appear to be in line with the VI's AML/CFT legislations. Many have additional policy documents that further outline TF and CDD related policies, processes and procedures. Over 90% of the legal practitioners have specific targeted financial sanction procedures such as screening and reporting. Most legal practitioners possess a general understanding of their TF risk as evident

by their policies, procedures, systems and controls they have in place such as reporting and screening in keeping with their TF obligations under the VI financial Sanction Guidelines 2023.

As it relates to the quality of reporting of suspicious transactions, between the period 2021-2023, 35 SARs were filed by 8 entities and it was indicated by the FIA-AIU that the quality of the SARs filed by the entities in this industry contained relevant information and provided valuable intelligence.

Between September 2024 – October 2024, FIA-SEU conducted and concluded an onsite inspection on ten legal practitioner firms for the period 2021 – 2023. Seven entities received an overall rating of Largely compliant due to adequate AML/CFT/CPF Policies, Procedures, systems and controls in place to mitigate ML/TF and PF risks such as, inter alia, adequate and updated institutional/ customer risk assessment, adequate CDD and ECDD measures, systematic and risk-based training, effective ongoing monitoring procedures, adequate TFS screening and monitoring measures and systems, proper record keeping procedures and effective reporting policies . Three entities indicated that they use introducers and comply with the relevant legislation by executing written agreements and testing of the relationship, where applicable. However, three of the entities attained an overall rating of partially compliant due to deficiencies within their AML/CFT policies, procedures, systems and controls which coincides with the findings of the initial desk-based review highlighted above. Some deficiencies include inadequate institutional and customer risk assessment, generic compliance programme which is not risk-based, inadequate CDD and ECDD measures, lack of an independent audit, poor implementation of their financial sanction's obligations. Therefore, in addition to remedial actions, the assessed entities were issued guidance documents in relation to institutional risk assessment, transaction monitoring, beneficial ownership and enhanced customer due diligence to provide further guidance to improve their AML/CFT/CPF measures and mitigate the risk of ML/TF and PF within their sector. However, most of the assessed entities are aware of their AML/CFT/CPF obligations given their affiliation with global entities with international standards. Sufficient training is provided to staff of most of the entities (especially the global firms) which is targeted and tailored and included testing.

Table 36 – Lawyers and Notaries Controls

CDD and EDD measures implemented	Entities carry out entity-level TFRA and implement corresponding controls.	Quality of Reporting of Suspicious Transactions	Employee training	Knowledge of TF and understanding of TF risk by the sector	Risk mitigation policies and procedures	TFS compliance	Overall control score
Satisfactory	**Satisfactory**	**Satisfactory**	**Good**	**Satisfactory**	**Satisfactory**	**Satisfactory**	**Satisfactory**

5.1.11 Real Estate Agents

Based on initial desk-based review 53% of the REAs have undertaken an institutional RA but have not carried out an entity-level TFRA. Therefore, although the REAs have AML/CFT/CPF policies and procedures in place which appear to be in line with the VI's AML/CFT Legislations, some appear to be generic and are not commensurate with their risk. They do not have clear policies as it relates to conducting CDD specifically to identify the BOs, and they do not include any specific policies or procedures for holding adequate, accurate and up to date information. Only a few of the REAs have specific targeted financial sanction procedures such as screening and reporting procedures. While no TFS specific inspections have been conducted over the last two years the 2024 onsite inspection had an area of focus as it relates to financial sanctions obligations. Most REAs possess a general understanding of their TF risk as evident by their policies, procedures, systems and controls they have in place such as reporting and screening in keeping with their TF obligations under the VI financial Sanction Guidelines 2023. Recordkeeping measures were found to be adequate as most REAs have indicated that they have record-keeping procedures and that they maintain records for 5 years. Between 2021 and 2023 only 1 SAR was filed by 1 entity.

Between September 2024 – October 2024, FIA-SEU conducted and concluded an onsite inspection on four real estates for the period 2021 – 2023. Each real estate agent received an overall rating of partially compliant due to deficiencies within their AML/CFT policies, procedures, systems and controls which coincides with the findings of the initial desk-based review highlighted above. Some deficiencies include inadequate institutional and customer risk assessment, generic compliance programme which is not risk-based, unsystematic and general training not specific to their sector and risk as well as, inadequate CDD and ECDD measures, lack of an independent audit and poor implementation of their financial sanctions

obligations as while the entities did have sufficient policies and procedures in relation to financial sanctions, they could not adequately demonstrate that screenings were being conducted systematically, at the start of the business relationship and on an ongoing basis. While the entities have a general understanding and knowledge of their AML/CFT obligations but there is much room for improvement. Therefore, in addition to remedial actions, the assessed entities were issued guidance documents in relation to institutional risk assessment, transaction monitoring, beneficial ownership and enhanced customer due diligence to provide further guidance to improve their AML/CFT/CPF measures and mitigate the risk of ML/TF and PF within their sector.

While the Real Estate sector conducted training within their respective organisations, the trainings were not risk-based, targeted, or tailored to the appropriate employee responsibility in keeping with the requirements of AMLTF Code. Additionally, although the training covered the broad AML/CFT/CPF obligations, the content was not substantial to demonstrate that the employees have an in-depth understanding of each AML/CFT/CPF obligation. For many of the entities a testing mechanism as outlined in section 48 of the AMLTF Code was not implemented to demonstrate that employees had a good understanding of their AML/CFT/CPF obligations. Additionally, in one instance, a real estate agent did not implement a systematic training programme which is not in keeping with Section 48 of the AMLTF Code which states that an entity should ensure that training be conducted for each employee at least once a year.

Table 37 – Real Estate Agent Controls

CDD and EDD measures implemented	Entities carry out entity-level TFRA and implement corresponding controls.	Quality of Reporting of Suspicious Transactions	Employee training	Knowledge of TF and understanding of TF risk by the sector	Risk mitigation policies and procedures	TFS compliance	**Overall control score**
Weak	**Weak**	**Weak**	**Satisfactory**	**Weak**	**Satisfactory**	**Satisfactory**	**Weak**

5.1.12 Dealers in Precious Metals and Stones

Based on an initial desk-based 65% of the DPMS sector have not undertaken an institutional risk or carried out TF specific RAs. Policies are generic and are not risk based. They do not

have clear policies in relation to conducting CDD specifically to identify the BOs, and they do not include any specific policies or procedures for holding adequate, accurate and up to date information. Only 60% of the DPMS have specific targeted financial sanction procedures such as it pertains to screening and reporting procedures. While no TFS specific inspections had been conducted over the prior two years, the 2024 onsite inspection had an area of focus as it relates to financial sanctions obligations.

A total of 2 DPMS were subjected to a CDD thematic examination in 2021 with both entities receiving a rating of partially and non-compliant respectively as it relates to their CDD policies and procedures. The record-keeping measures are adequate as most DPMS have indicated that they have record-keeping procedures and that they maintain records for 5 years. Most DPMS possess a general understanding of their TF risk as evident by their policies, procedures, systems and controls they have in place for reporting and screening in keeping with their TF obligations under the VI financial Guidelines 2023. Between 2021 and 2023 no SARs were filed by the DPMS sector.

Although the trainings conducted covered the broad AML/CFT/CPF obligations, there were deficiencies: The trainings were not risk-based, targeted, or tailored to the appropriate employee responsibility in keeping with the requirements of AMLTF Code. Some of the training was not designed to test employee's knowledge of money laundering, terrorist financing and proliferation financing pursuant to section 48 of the AMLTF Code. And therefore, the entities were not able to adequately demonstrate that that employee had a good understanding of their AML/CFT/CPF obligations.

Table 38 – Dealers in Precious Metals and Stones Sector Controls

CDD and EDD measures implemented	Entities carry out entity-level TFRA and implement corresponding controls.	Quality of Reporting of Suspicious Transactions	Employee training	Knowledge of TF and understanding of TF risk by the sector	Risk mitigation policies and procedures	TFS compliance	Overall control score
Weak	**weak**	**Weak**	**Satisfactory**	**Weak**	**Satisfactory**	**Satisfactory**	**Weak**

5.1.13 High Value Goods Dealers

Based on an initial desk-based review 62% of the registered HVGDs appear to have not undertaken an institutional RA and therefore, their policies and procedures are not risk-based. Therefore, although the HVGD have AML/CFT/CPF policies and procedures in place which appear to be in line with the VI's AML/CFT Legislations, they are generic and do not commensurate with their risk. They do not have clear policies as they relate to conducting CDD specifically to identify the BOs, and they do not include any specific policies or procedures for holding adequate, accurate and up to date information. Only 70% of the HVGDs have specific financial sanctions procedures such as it pertains to screening and reporting procedures. Although, no TFS specific inspections have been conducted over the last two years the 2024 onsite inspection had an area of focus as it relates to financial sanctions obligations.

The recordkeeping measures are adequate as most HVGD have indicated that they have record-keeping procedures and that they maintain records for 5 years.

Most HVGDs possess a general understanding of their TF risk as evident by their policies, procedures, systems and controls they have in place which include reporting and screening obligations, which are in keeping with the VI Sanctions Guidelines. Between 2021 and 2023 no SARs were filed by the HVGD sector.

Between September 2024 – October 2024, FIA-SEU conducted and concluded an onsite inspection on four HVGD for the period 2021 – 2023. Each DPMS received an overall rating of partially compliant due to deficiencies within their AML/CFT policies, procedures, systems and controls which coincides with the findings of the initial desk-based review highlighted above. Some deficiencies include inadequate institutional and customer risk assessment, generic compliance programme which is not risk-based, unsystematic and general training not specific to their sector and risk as well as , inadequate CDD and ECDD measures, lack of an independent audit and poor implementation of their financial sanctions obligations as while the entities did have sufficient policies and procedures in relation to financial sanctions, they could not adequately demonstrate that screenings were being conducted systematically, at the start of the business relationship and on an ongoing basis. While the entities have a general understanding and knowledge of their AML/CFT obligations but there is much room for improvement. Therefore, in addition to remedial actions, the assessed entities were issued

guidance documents in relation to institutional risk assessment, transaction monitoring, beneficial ownership and enhanced customer due diligence to provide further guidance to improve their AML/CFT/CPF measures and mitigate the risk of ML/TF and PF within their sector.

While the HVGD sector conducted training within their respective organisations, the trainings were not risk-based, targeted, or tailored to the appropriate employee responsibility in keeping with the requirements of AMLTF Code. Additionally, although the training covered the broad AML/CFT/CPF obligations, the content was not substantial to demonstrate that the employees have an in-depth understanding of each AML/CFT/CPF obligation. For many of the entities a testing mechanism as outlined in section 48 of the AMLTF Code was not implemented to demonstrate that employees had a good understanding of their AML/CFT/CPF obligations.

Table 39 – High Value Good Dealer Controls

CDD and EDD measures implemented	Entities carry out entity-level TFRA and implement corresponding controls.	Quality of Reporting of Suspicious Transactions	Employee training	Knowledge of TF and understanding of TF risk by the sector	Risk mitigation policies and procedures	TFS compliance	**Overall control score**
Weak	**Weak**	**Weak**	**satisfactory**	**Weak**	**Satisfactory**	**Satisfactory**	**Weak**

5.2 Legal Persons and Arrangements Controls

As a detailed and targeted RA of LPLAs and their ML, TF and PF risk in the VI took place in 2024, this enabled current and accurate data to be utilised and considered in relation to TF risk. The LPLA RA concluded that overall controls were satisfactory.

In relation to general controls, in the VI, nominee shareholders must disclose their status to the registered agent of the legal person for which they act as nominee. ROCA does not currently verify the accuracy of BO information provided and does not impose penalties for failure to provide or update BO information. Recent legislative changes have now made this a requirement, and processes are currently being put into place to allow for the maintenance of this information. The FSC, however, does require TCSPs to maintain BO information on their clients in keeping with AML/CFT legislation and this requirement is tested through the FSC's

compliance inspection process and penalties are imposed for failure to maintain adequate, accurate and up to date BO information. The concept of nominee director does not exist in the VI. Bearer shares are prohibited. Therefore, this was assessed as satisfactory because the BO registry and related legislative changes are not yet in force.

As it relates to access to information, the following factors were assessed: LEAs and competent authorities can access basic and BO information on a timely basis, while foreign authorities can access basic and BO information through the normal information exchange channels. Authorities can exchange information on shareholders and there is an avenue for foreign counterparts to access BO information, as agencies responsible for responding to international requests are publicly known, FIs and DNFBPs in the country can access basic information on a timely basis. The assessment revealed that LEAs, competent authorities, FIs and DNFBPs can always access the information listed above on a timely basis. The rating on this factor was Good.

The LPLA RA also considered the compliance levels of entities in gatekeeper roles, including TCSPs and legal professionals, with AML/CFT requirements, as gatekeepers that are compliant with AML/CFT obligations can detect bad actors and prevent them from operating a legal person or legal arrangement in the VI.

For FIs and TCSPs, compliance with controls was rated as generally good or satisfactory, except for ongoing monitoring and reporting of suspicious activities, which were rated as weak. Overall, the level of compliance for this group is satisfactory. The compliance level of the legal and accounting professions was weaker than for TCSPs and FIs. The compliance of the legal profession was rated as weak or very weak on the issues of business RAs, CDD measures, reliance on third parties, internal controls and SAR filings. The accounting profession was assessed as having the same weaknesses as the legal profession with the addition of weakness in ongoing monitoring. Overall, the level of compliance for this group was found to be weak.[108] As this area was considered separately in the LPLA Risk Assessment, the table of residual risk scores was also considered there and is located below. (As can be seen from the table the

[108] Given that TCSPs and FIs are more likely to be involved in company formation and ongoing monitoring than lawyers and accountants, the satisfactory rating for FIs and TCSPs was given more weight than the rating for lawyers and accountants, for an overall rating of satisfactory on this factor.

residual risk for legal arrangements is ML, the controls were found to be satisfactory, and the main weakness was in the controls is the compliance of the FIs and DNFBPs with their regulatory obligations.

Table 40 – Residual Risk Scores[109]

	TF
BVIBC - Limited by Shares	MH
BVIBC - Limited by Guarantee (shares)	ML
BVIBC - Limited by Guarantee (non-shares)	MH
Unlimited Company	MH
Unlimited company (non-shares)	ML
Segregated Portfolio Company	ML
Restricted Purpose Company	ML
Private Trust Company	ML
Limited Partnership	ML
International Partnership	ML
Partnership without Legal Personality	ML
Foreign companies	ML
Vista Trusts	ML
Express Trusts	ML

5.3 NPO Controls

As indicated above, a sectorial RA of NPOs and their TF risk was concluded in August 2024, and this enabled the current assessment of TF of the NPO sector in the VI to be considered. The NPO RA concluded that controls were adequate given the low level of TF threat and abuse but not risk-based.

While the NPOs' policies and procedures are in keeping with some aspects of FATF Recommendation 8, they are applied to all NPOs in the VI. Therefore, a risk-based approach must be adopted to ensure the measures are commensurate with the risks identified.

[109] Table 13, of the LPLA RA 2025

Additionally, these measures should be CFT focused and in line with Recommendation 8 in order to effectively mitigate TF risks within the NPO Sector.

Further, it is apparent that further CFT training and awareness is required among the NPO sector, especially for the higher risk NPOs, in order to promote accountability, integrity and public confidence in the administration and management of NPOs through improvement and development of the relevant policies and procedures. Furthermore, a collaborative effort is necessary to ensure that NPOs develop and refine best practices to address TF risk and vulnerabilities and thus protect them from TF abuse.

While there exist inherent vulnerabilities within the NPO sector and deficiencies in the legislative framework, the overall inherent risk is assessed as low due to the low level of TF threat and abuse. However, both public and private stakeholders play a pivotal role in ensuring that these vulnerabilities are not exploited for TF and other illicit purposes

In accordance with the AML Code, NPOs in the VI are required to implement policies, procedures, systems and internal controls which promote accountability and integrity and mitigate the risk of money laundering, TF and proliferation financing. Based on the data collected, 56% of faith based NPOs claimed that they have the relevant policies and procedures in place via their constitution, bylaws or articles of incorporation, standard code of conduct and internal code of polices for transparency and accountability with 19% possessing an AML/CFT compliance manual. Most of the NPOs in the VI do not possess an AML/CFT compliance manual and therefore do not have adequate CFT Policies governing their organisation.

In relation to the adequacy of internal policies and procedures, Charitable NPOs are the main NPOs that cross-check the name of their staff, donor or volunteers against the UN sanction list, UK Office of Financial Sanctions Implementation website, and the US OFAC list. Only 6.25% of the Religious NPOs cross reference the name of their staff, donors or volunteers with designated individual and entities on the UN Sanctions List as the NPOs claimed that most of their donors and staff are members or known individuals with a connection to the religious organisation. However, 56.25% of the Religious NPOs engage in basic vetting procedures for donors which include name, address and source of funds and may request the completion of a membership form or the donor's licencing certificate for verification purposes. Whilst most of the NPOs claimed that they are not aware of whether their donors are PEPs or have CFT

policies, the international donors that provide funding to these organisations are not located in high-risk jurisdictions, or in proximity to countries with an active terrorist threat.

Over 95% of the NPOs indicated that all transactions are recorded either manually, electronically or both for an average period of 5 to 7 years. Additionally, 56% of the Religious NPOs claimed that they review the transactions for suspicious patterns of activity per activity or monthly during their bank reconciliation period. Moreover, over 90 % of the FATF NPOs indicated that they have completed and submitted annual financial statements to the NPO Board which facilitate a level of transparency and accountability.

5.4 Controls Relating to the Use and Movement of Cash and Dealers in Precious Metals and Stones

In relation to controls specific to the use of cash, the ability of HMC to detect incoming and outgoing movement of cash and to take action was considered. Additionally controls on the use of cash within the regulated sectors were also considered. The legislative framework is in place to detect illicit cash and PM&S, and the controls were found to be satisfactory.

5.5 Controls - Public Sector

The controls in effect in the public sector as it relates to supervision were rated as satisfactory. To reach this conclusion, an assessment was made in relation to public sector (and regulator) activity, monitoring and enforcement including the percentage of the sector subject to an offsite inspection over the last 2 years including the percentage of higher risk entities within the sector that were subject to an offsite and / or onsite examination. The level of enforcement action taken in relation to each sector as it relates to TF was also considered. The adequacy of the resources of supervisors to adequately monitor the implementation of counter TF measures within each sector was also taken into account as well as the expertise and training of the public sector. The level of industry engagement relating to TF was also assessed.

5.5.1 The Financial Services Commission

The FSC's Regulatory division consists of the Authorisation and Supervision Division (ASD), the Enforcement Division, the Compliance Inspection Unit and the AML Unit. The ASD consists of four Units: Authorisation, Specialised Supervision, Prudential Supervision and

Market Conduct[110]. The Authorisation Unit (AU) consists of one Deputy Director, three Senior Regulators and thirteen Regulators I/II. The AU is the centralised unit responsible for authorisation and cessation activities of all regulated persons and receives and processes all pre-licencing and post-licencing applications for consideration and potential approval. The AU's function is to ensure that all applicants and existing regulated entities satisfy the requirements to carry out regulated activities. On average, the AU processes approximately one hundred and thirty-four applications monthly.

The Prudential Supervision Unit (PSU) consists of one Deputy Director, two Senior Regulators and ten Regulators I/II. The PSU is responsible for monitoring and supervising regulated entities that present a lower level of risk to the financial services sector.[111] There are currently 600 licenced entities under PSU's portfolio.

The SSU consists of one Deputy Director, two Senior Regulators and seven Regulators I/II. Its function is to monitor and supervise systemically important financial institutions and other regulated entities with a higher level of risk. The SSU is responsible for undertaking proactive and enhanced supervision of these entities. There are currently 124 licenced entities across the banking (7), MSB (2), Financing (3), TCSP (93), IB (11), Insurance (6) and VASP (9) sectors under SSU's portfolio.[112]

The Enforcement Division consists of one Deputy Director (vacant), two Senior Enforcement Officers and four Enforcement Officers I/II. Its function is to lead on taking enforcement action against licencees and unauthorised persons who commit breaches of relevant laws. The ED is responsible for conducting investigations, monitoring and presenting all matters relating to contraventions to the FSC's Enforcement Committee for consideration of enforcement action. The ED receives and analyses intelligence on behalf of the FSC and conducts investigations of serious breaches of financial services legislation. Its investigative work ranges from regulatory breaches, such as entities engaging in unauthorised financial services activity, to cases where non-regulated BVI Business Companies are being used for unlawful purposes.

[110] The Market Conduct Unit consists of one prudential conduct manager and one Regulator. MCU's function is to promote a fair and transparent market in which all stakeholders within the financial services industry are treated fairly, honestly, and professionally.
[111] It is also responsible for reviewing and processing all post-licencing filings required to be submitted by existing regulated entities and regulated persons.
[112] As of November 2024.

The Compliance Inspection Unit (CIU) consists of one Deputy Director, four Senior Regulators, four Regulators Is, four Regulator IIs and 1 Administrative Assistant. The CIU's mandate is to undertake onsite reviews of licencees across all sectors through the planning, preparing and conducting of onsite inspections. The primary focus of the CIU is AML/CFT and prudential inspections. The CIU undertakes full scope and/or thematic examinations of specific entities or sectors based on identifiable risks and assesses licencees levels of compliance with requirements of relevant financial services legislation.

The AML/CFT Unit consists of one Deputy Director, two senior level analysts and one junior analyst and is responsible for developing and implementing the FSC's AML/CFT supervisory and regulatory strategy and policy and keeping abreast of AML/CFT international standards and advising the FSC on how to incorporate changes into the regulatory framework to ensure the jurisdiction's compliance with such standards. The AMLU is also responsible for the monitoring of international sanctions and other restrictive measures, while providing key stakeholders with relevant information and guidance to promote integrity and stability within the financial services industry in the VI.

Training

All FSC regulatory staff are subjected to mandatory AML/CFT introductory training and annual AML/CFT training. A majority of regulatory staff have achieved relevant AML/CFT qualifications such as those issued by ICA and CAMs. Staff from, ASD, AMLU, Compliance Inspections Unit and the Enforcement Division have participated directly in CFT training related to investigating TF, how to identify TF, and use of VAs in TF. This training included sessions facilitated by OFSI, FCDO, ACAMS and RSS Asset Recovery. In addition, the FSC is a member of the OT's TF Forum which meets bi-annually and provides participants with the opportunity to discuss emerging TF risks and trends and share best practices. It also participates in the annual FCDO Sanctions Forum. In March 2024 the FSC participated in a multi-agency sanctions tabletop exercise sponsored by the FCDO, which included elements of TF. In June 2024 staff also attended a multi-agency workshop on TF and TFS. Staff have also received FATF assessor and standards training which has aided in enhancing the understanding of their CFT obligations as a regulator of financial services.

Publications/Guidance

In 2021, the FSC published the findings of the 2020 ML and TFRA for the MSB Sector. In 2022, the FSC produced a 20-minute video, which provided viewers with information on TFS and discussed their obligations in relation to, amongst other things, screening and reporting. This video has garnered 343 views. In addition, the Virgin Islands Sanctions Guidelines, which cover TFS for TF were updated and re-issued in 2023. In 2024, as part of a collaborative outreach effort between various public sector agencies and private sector associations, the Sanctions Coordinator within the AGC delivered a presentation to 262 industry professionals on their sanctions obligations with regard to implementing and enforcing TFS including those relative to TF.

Banks, Money Services Business, Insurance, Insolvency and Financing

Over the last two years, all banks have been subjected to ongoing desk-based reviews which include reviews of AML/CFT returns, prudential returns and compliance officer reports which address AML/CFT issues. This means all higher risk banks have been reviewed offsite during this period. In relation to onsite inspections, two of the seven banks (29%) have been inspected within the past two years. Furthermore, 100% of the banking inspections were conducted at the banks that presented the highest risks within the sector. All inspections for Banks are full scope and encompass a TFS review and assessment. It is expected that all seven banks will be inspected by the end of 2025. During the reporting period there were no instances where enforcement action needed to be taken against any licencee within the banking sector. AML/CFT Guidelines for the Banking sector were issued in July 2020. In 2021, the FSC published the findings of the 2020 ML and TFRA for the Banking Sector.

Although one MSB is risk-rated as L and the other ML for ML/TF risk, due to the cash intensive nature of MSB, for supervisory purposes, both are classified as systematically important and subject to specialised supervision by the FSC. As such all MSBs were subject to desk-based and ongoing supervision between 2022 and 2023. In addition to desk-based monitoring, 50% of MSBs were subject to onsite inspection between 2022 and 2023. No instances requiring enforcement action needed to be taken within the MSB sector during the reporting period. AML/CFT Guidelines for the MSB sector were issued in 2016. In 2021, the FSC published the findings of the 2020 ML and TFRA for the MSB Sector.

Fifty-two insurance licencees (insurers and intermediaries) (29%) have been subject to desk-based reviews between 2022 and 2023. All higher risk entities were subjected to review. No inspection of insurers or insurance intermediaries between 2022 and 2023 included TFS given the identified low risk. No AML/CFT breaches including TFS related breaches requiring enforcement action needed to be taken within the insurance sector during the reporting period. In 2021, the FSC published the findings of the 2020 ML and TFRA for the Insurance Sector.

Given the low-risk nature of insolvency work, no IPs were subject to inspection (onsite or offsite) over the last 2 years. Further, there were no instances where enforcement action needed to be taken against any licencee within the insolvency sector during the reporting period.

All FBs underwent desk-based reviews during the reporting period. However, there have been no onsite inspections of FB licencees over the last three years due to the low level of risk posed. During the reporting period there were no instances where enforcement action needed to be taken against any licencee within the financing sector. In 2021, the FSC published the findings of the 2020 ML and TFRA for the Financing Sector.

Table 41 - Controls: Regulation of Banks, Money Services Businesses, Insurance, Financing and Insolvency:

Percentage of sector (including high risk) subject to offsite over last 2 years	Percentage of sector (including high risk) subject to onsite over last 2 years	Enforcement action	Resources of supervisors	Industry engagement	Knowledge of CFT obligations by public sector (expertise and training)	**Overall public control score taking into account weight of factors**
Good	**Good**	**Good**	**Good**	**Good**	**Good**	**Good**

Investment Business

As it relates to IB, all higher risk entities are subjected to review through desk-based assessments as part of the FSC's risk-assessment framework. At the end of 2023, five IBs

(2.17% of the IB sector), accounting for 22 categories of licence collectively were considered 'higher risk' having received a risk rating of MH (20) or H (2) and are under the supervision of the FSC's SSU. These entities have relationship managers who assess the level of risk annually and on an ongoing basis. Between 2022 and 2023 sixty-seven IB licencees were subject to desk-based review. Thirteen IB licencees have been subject to on-site inspections between 2020 and 2023. Five of the thirteen IB licencees reviewed onsite were higher risk licencees, supervised by the specialised supervision unit. However, no inspection of IB licencees between 2022 and 2023 included TFS. The total number of IB inspections carried out represents 9.98% of the IB Sector and 45% of the IB licencees under the remit of the Specialised Supervision Unit. There are 16 IB inspections scheduled for 2024 that will include a review of licencees' systems, policies and procedures for handling TFS and effectiveness of such systems.

Table 42 - Controls: Supervision of Investment Businesses

Percentage of sector (including high risk) subject to offsite over last 2 years	Percentage of sector (including high risk) subject to onsite over last 2 years	Enforcement action	Resources of supervisors	Industry engagement	Knowledge of CFT obligations by public sector (expertise and training)	**Overall public control score taking into account weight of factors**
Good	**Satisfactory**	**Good**	**Good**	**Satisfactory**	**Good**	**Satisfactory**

Virtual Assets Service Providers

VASPs came under the FSC's supervisory remit in 2023, with the first licence being issued in 2024. As such, no inspections have been carried out yet, nor have there been any instances where enforcement action has needed to be taken against any VASP licencee. The FSC has adopted a comprehensive approach to licencing and supervision, including providing clear and detailed guidance to entities during the onboarding process, conducting detailed assessments of each entity's current practices, identifying areas requiring modification, and providing tailored guidance to facilitate the transition.

In 2023, the FSC issued specific AML/CFT Guidelines for VASPs. In addition, as part of its continual outreach efforts, during its October 2023 Meet the Regulator Forum the FSC presented to the industry on VASP Processes and Procedures. This event was attended by approximately 300 persons. The FSC also published its Virtual Assets Service Providers' AML Guidelines: A Tool for Demonstrating Compliance in 2024. In addition, an article was published in the March 2024 issue of the FSC's newsletter focused on the findings of the 2022 MLRA relative to the higher-risk TCSP, VASP and IB sectors. Additionally, the FSC issued guidance on the VASP Travel rule during the review period.

Table 43 - Controls: Supervision of VASPs

Percentage of sector (including high risk) subject to offsite over last 2 years	Percentage of sector (including high risk) subject to onsite over last 2 years[113]	Enforcement action	Resources of supervisors	Industry engagement	Knowledge of CFT obligations by public sector (expertise and training)	**Overall public control score taking into account weight of factors**
Satisfactory	**Weak**	**Weak**	**Satisfactory**	**Satisfactory**	**Good**	**Satisfactory**

Trust and Corporate Service Providers

Higher risk TCSPs are subjected to review through desk-based assessments as part of the FSC's risk-assessment framework. These entities have relationship managers who annually, and on an ongoing basis, assess the level of risk. At the end of 2023, seven TCSPs (2.4%) were considered 'higher risk' having received a risk rating of MH (5) or H (3) and are under the supervision of the FSC's SSU. Thirty-seven TCSPs (13%) have been subject to onsite inspections between 2020and 2023. Of the thirty-seven TCSPs inspected, 18 (49%) were higher-risk entities that fall under the FSC's specialised supervision regime.

[113] The activity was not subject to licencing until 2024, therefore entities were not subject to onsite inspection during the reporting period.

Between 2020 and 2023, nine TCSPs, rated as Higher Risk, were subject to an on-site inspection. This accounted for 41% of all licencees rated as higher risk. Three of the nine inspections conducted were full scope inspections, which aimed to understand the implementation and effectiveness of the licencees' ML/TF compliance framework. The remaining six inspections were thematic and focused on areas that posed higher ML/TF risk, such as Enhanced Due Diligence **(EDD)** and Sanctions Handling. It should also be noted that the onsite inspection strategy isolates and considers the ML/TF risk score. As such, all thematic inspections conducted during the period of 2020 – 2023 generally focused on those TCSPs with elevated ML/TF risk scores.

During the reporting period various enforcement actions were taken within the TCSP sector. Actions included the issuance of warning letters, directives and public statements, as well as the revocation of 5 licences and the imposition of $1,063,500 in administrative penalties, $450,000 of which related to AML breaches. None, however, were as a result of any TF or TFS breaches. In 2023, the FSC issued AML/CFT specific guidance for TCSPs. An article was also published in the March 2024 issue of the FSC's newsletter focused on the findings of the 2022 MLRA relative to the higher-risk TCSP, VASP and IB sectors.

Table 44 - Controls: Supervision of Trust and Corporate Service Providers

Percentage of sector (including high risk) subject to offsite over last 2 years	Percentage of sector (including high risk) subject to onsite over last 2 years	Enforcement action	Resources of supervisors	Industry engagement	Knowledge of CFT obligations by public sector (expertise and training)	**Overall public control score taking into account weight of factors**
Satisfactory	**Satisfactory**	**Good**	**Good**	**Good**	**Good**	**Satisfactory**

The rating for public sector controls regarding supervision by the FSC was good for regulation of Banks, MSBs, Insurance, Financing and Insolvency, and satisfactory for TCSPs, Investment Business and VASPs, when the materiality and risk of these sectors was considered, the overall rating was satisfactory.

5.5.2 Financial Investigation Agency Supervision

The FIA-SEU supervises legal practitioners and accountants undertaking relevant business in accordance with the AMLRs, REAs, HVGDs, DPMS, and NPOs. The FIA-SEU consists of one Deputy Director, one Chief Compliance Examiner, one Senior Compliance Examiner, two examiners, and three junior compliance examiners currently undergoing training. Each individual is equipped with two PCs which facilitate efficiency as well as access to websites such as FATF e-learning and ECOFEL to facilitate developing knowledge in AML/CFT/CPF. While some staff have attained training in CFT and TFS at different levels, further training is required as this area is new to most. The FIA-SEU has completed onsite examination of 25 entities which provided a greater understanding of the adequacy of the AML/CFT/CPF policies, procedures, controls and systems their supervised entities have in place to combat ML/TF/PF risks inclusive of their level of TFS compliance No enforcement action has been taken in relation to TF matters for the period 2021-2023.

Over the past 3 years, the VI has provided the following TF-specific guidance: The Virgin Islands Sanctions Guidelines 2023, Guidance Notes on Terrorist Financing Risk and Red flags for NPOs 2023 and sector specific guidance on 'What is terrorist financing?' for legal practitioners and Accountants, REAs / jewellers / DPMS, Boat and Yacht Brokers and Vehicle Dealers. For the last 2 years, the FIA-SEU has not conducted any inspections within the accounting sector.

The FIA-SEU did not conduct full inspections for the Legal Practitioner sector in 2022 or 2023. A total of seven legal practitioners were subject to CDD thematic examination in 2021 and received a non-compliant rating for major deficiencies in their CDD processes and procedures.

Between 2022 and 2023, the FIA-SEU did not conduct any full scope inspections within the real estate sector. A total of four real estate agents were subject to CDD Thematic examination in 2021 with two entities receiving a largely compliant rating for their CDD policies and procedures.

In 2022 and 2023, the FIA has not conducted full inspections with the DPMS sector. A total of two DPMS were subject to CDD Thematic examination in 2021 with two entities receiving a rating of partially and non-compliant respectively as it relates to their CDD policies and procedures.

In 2022 and 2023 years, the FIA has not conducted full inspections with the HVGD sector. A total of six HVGD were subject to CDD Thematic examination in 2021 with most of the entities receiving a rating of non-compliant in relation to their CDD policies and procedures.

However, in 2024 the FIA-SEU carried out a number of onsite inspections as detailed above.

Table 45 - Regulatory Controls in Relation to Lawyers and Notaries, Accountants, Real Estate Agents, Dealers in Precious Metals and Stones and High Value Goods Dealers

Percentage of sector (including high risk) subject to offsite over last 2 years	Percentage of sector (including high risk) subject to onsite over last 2 years	Enforcement action	Resources of supervisors	Industry engagement	Knowledge of CFT obligations by public sector (expertise and training)	**Overall public control score taking into account weight of factors**
Satisfactory	**Satisfactory**	**Weak**	**Weak**	**Satisfactory**	**Satisfactory**	**Satisfactory**

The conclusion of controls as it relates to the FIA Supervision was satisfactory.

5.5.4 Controls – Law Enforcement, Financial Investigation Agency - Analysis and Investigation Unit, Director of Public Prosecutions and Attorney General's Chambers:

The extent to which law enforcement provided an effective control was also considered. Each Law Enforcement or related agency was considered, namely RVIPF-intelligence, RVIPF FCU and the remaining RVIPF units. HMC and DOI were also assessed as well as the FIA-AIU and the ODPP. The level of enforcement action taken[114] was considered, as well as the available resources of the LEAs[115]. The expertise and training[116] of the LEAs as it relates to TF was also considered. For each LEA a rating was allocated. These were then combined to

[114] *Enforcement action is taken as required in relation to TF matters: Good
*Enforcement action is taken in most cases where it is required in TF matters: Satisfactory
*There is insufficient enforcement for TF breaches: Weak
*There is no enforcement where TF breaches or offences occur: Very weak
[115] *Resources are sufficient: Good
*Some improvement needed: Satisfactory
*Difficult to complete TF mandate with current staff levels; *Weak - Cannot complete TF mandate with current staff levels: Very Weak
[116] *Sufficient staff have expertise in TF and / or training in TF.
*Reasonable levels but some improvement needed. Satisfactory
*Some experience and training but insufficient to complete TF mandate: Weak
*No staff with TF expertise or training: Very Weak

deduce the overall rating for the extent to which law enforcement operated as an effective control in reducing TF risk.

The FIA-AIU attended four training sessions in 2022 and 2023 geared towards CFT and has obtained two new analysts experienced in VAs as well as virtual asset software which assists in its analysis of VA related matters. The FIA-AIU considers that it has adequate resources to deal with the Territory's TF risk.

The RVIPF-FCU had insufficient resources during the period 2020 to 2023. However, the agreed new staffing levels for the FCU Team are nine Detective Constables, a Financial Analyst, two Detective Sergeants and a Detective Inspector. At the time of the RA the posts had received funding, but had not all been filled. As the RVIPF-FCU is fundamental to the investigation and onwards prosecution of TF matters this matter was given additional weight above CFT knowledge, although the FCU officers who are in place have had TF training, it is anticipated that due to the changes agreed in 2024, once positions are filled, this deficiency will be remediated. The officers of the FCU have received the following training: Sanctions Breach training hosted by the UK Financial Intelligence Unit and the UK Sanctions Directorate, TF tabletop exercise, Investigation of Terrorist Financing practical exercise for one week and attendance at the Overseas Territories TF Forum. Additional Training has been confirmed, namely the National Crime Agency training on: Financial Intelligence, Financial Investigation, Restraint, Confiscation, Senior Appropriate Officer and Cryptocurrency. Enhanced case management has been implemented to measure performance of investigations into TF. Technical resources have been budgeted for. These tools are vital for a Financial Crime Unit to function effectively. These include a system and software for financial analysis for the Financial Analyst. A crypto analytical software to assist with virtual asset investigation including blockchain analysis at the time of the risk assessment was in the procurement phase.

The FCU has issued new policies in relation to international cooperation and intelligence sharing (September 2024) and The Investigation of Legal Persons and Legal Arrangements (finalised and circulated in September 2024). Additionally, the FCU has initiated a new procedure utilising Collaborative Law Enforcement Agencies (CLEA), whereby TF risks and trends are monitored and brought to the attention of CLEA members. A TF Trends and Typologies policy was also finalised and circulated in September 2024. At the time of the RA

the FCU was leading the TF investigation and prosecution strategy, to be completed in Q1 2025.

A Memorandum of Understanding between the RVIPF FCU and the FIA-AIU has been updated to reflect and prioritise TF investigations and suspected sanctions breaches. Feedback is to be provided on the quality of intelligence provided. The monitoring of investigations and timescales for the provision of intelligence has been adopted. Operational and Strategic meetings take place at monthly and quarterly intervals respectively.

RVIPF Intelligence is undergoing a review of the IU in relation to the Law Enforcement Review. The new structure will allow for better sharing of information with the analysts that will be based within the RVIPF FCU and there will be some ongoing intelligence gathering in relation to VAs and informal transfer services. The Intelligence Officers will be trained in processing and developing TF intelligence received. RVIPF Intelligence was unable to provide relevant data or analysis and stated that there was insufficient training on terrorism or TF. Requests in relation to financial matters were sent to FIA-AIU where they were dealt with, but RVIPF Intelligence was not able to provide further information on these requests or responses to them or indeed in relation to requests which did not go to FIA-AIU. It was noted that there was little capability or capacity within the unit to undertake any financial intelligence development or analysis. It was also noted that no financial or TF training had been undertaken.[117]

Whilst there have not been any terrorism or TF cases during the review period, the ODPP underwent specialised training in October 2024 and January 2025 which included the prosecution of TF cases. An expansion of the ODPP is also underway which will increase capacity in all financial crime matters including TF through the creation of a Financial Unit within the ODPP, for which Crown Counsel and Senior Crown Counsel had been put in place and additional recruitment was budgeted for and underway.

The AGC-IC has adequate resources to deal with requests relating to Terrorism and TF, namely one dedicated Crown Counsel, with two additional Crown Counsel, one dedicated Case Manager and one Legal intern. The International Relations Counsel has received TF training

[117] One officer had completed online seminars in relation to Crypto Currencies.

from CFATF and Senior Crown Counsel leading the ICT in the AGC gained knowledge while pursuing an LLB in Financial Crimes Regulations and cryptocurrency certification.

The DOI's organisational structure in 2024 entails a total of 77 persons employed across the various units of the department. There are currently 54 Immigration Officers within the Border Management Unit, who are assigned to ports of entry across the VI, whose main function is to perform inspections of persons entering and departing the Territory. There are 13 members of staff within the DOI's Administration Unit and 10 officers within the Enforcement Unit. Therefore, the DOI remains drastically understaffed in all units. It is anticipated that in 2025 a further four Enforcement Officer posts will be funded to further augment work in areas related to enforcement, compliance, investigations and monitoring in TF and TFS matters. Currently, only members of the Enforcement Unit, the senior management team and a few immigration officers have been trained in TF and TFS and have general knowledge of the subject area. In June 2024, five officers from DOI's Management and Enforcement Unit attended TF and TFS Training. In 2020, the DOI upgraded its border management system from the non-operational Entrex system to the advanced Border Management and E-Visa System. Enforcement officers utilise the system to analyse travel patterns, particularly focusing on movement to and from high-risk jurisdictions. The system has proven effective not only in identifying potential entrants from high-risk areas but also in tracking those who have successfully entered the territory for purposes such as employment or residency over the reporting period.

65 Officers are currently active in HMC. 130 Officers are needed to adequately carry out the tasks of the HMC. No improvement has been made since 2017 to improve staffing efficiency. Before hurricane Irma, the department had approximately 110 Officers. Only a handful of officers are knowledgeable of TF and TFS. Hiring of staffing is in progress. TF training was undertaken in 2021, and the Financial Crime Investigation Training Course was attended in July 2024. A Risk Management Unit is to be created that will focus, amongst other things, on TF related matters. HMC has engaged The Caribbean Regional Technical Assistance Centre (CARTAC) is in the process of implementing a RA group, which will give the department the ability to assess/track movements of persons/goods with links to TF high risk countries and utilising the VI as a transit points.[118] With collaboration with the other jurisdictions this will give HMC the ability to intercept the movement of cash by utilising intelligence-led operations.

[118] HMC also noted that the incorporation of risk management in legislation was being considered.

Each of the individual ratings was considered as well as their weighting, particularly in relation to resources at the RVIPF-FCU which is fundamental to the investigation and ultimate prosecution of TF matters in line with the risk profile of the jurisdiction. Whilst additional resources have been allocated, they were not yet in place at the time of this risk assessment and therefore the overall conclusion was that the rating of weak was appropriate for the law enforcement controls.

Table 46 - Summary of Control Ratings for Law Enforcement, Financial Investigation Agency - Analysis and Investigation Unit, Director of Public Prosecutions and Attorney General's Chambers

	Enforcement Action	**Resources of LEAs**	**Knowledge of CFT obligations**	**Overall rating of agency**
RVIPF-Intel	NA	Weak	Weak	Weak
HMC	Good	Weak	Satisfactory	Satisfactory
DOI	Good	Weak	Satisfactory	Satisfactory
FCU	Weak	Very Weak	Satisfactory	Very weak
RVIPF-Other	Weak	Very Weak -	Very Weak	Very Weak
FIA-AIU	Good	Satisfactory	Good	Good
AGC IC	NA	Good	Good	Good
DPP	N/A	Weak	Good	Satisfactory
Overall rating of law enforcement controls		Weak		

5.6 Conclusion Regarding Controls

Table 47 - Control ratings

Area	**Rating**
Banking	Good

MSBs	Good
Insurance Business	Good
Financing	Good
Insolvency	Good
Investment Business	Satisfactory
VASPs	Satisfactory
TCSPs	Satisfactory
Lawyers and Notaries	Satisfactory
NPOs	Satisfactory
Use and movement of cash	Satisfactory
Public sector controls – supervision by FSC	Satisfactory
Legal persons and arrangements	Satisfactory
Public sector controls – supervision by FIA SEU	Satisfactory
Accountants	Satisfactory
Public sector controls – law enforcement and related agencies	Weak
DPMS	Weak
HVGD	Weak
Real Estate	Weak

6. Residual Risk

In order to reach a determination in relation to the risk of the collection, movement and use of terrorist funds in the VI as well as the risk of each typology being utilised for the purposes of TF, the controls, namely private sector controls, public sector controls and law enforcement controls were applied to the likelihood rating in order to determine the overall residual risk rating.

Table 48 - Chart Used to Calculate Residual Risk

Likelihood	**Controls:**	Good	Satisfactory	Weak	Very Weak
L		L	L	L	L

ML	L	ML	ML	ML
MH	ML	MH	MH	MH
H	MH	H	H	H

Table 49 – Calculating Residual Risk

Typology	Threat Rating	Relevant sectors	Overall vulnerability	Likelihood rating	Private Sector control rating	Public sector control rating[119]	Overall Residual Risk Rating for typology
Typology 1	MH	TCSPs Legal persons	MH MH	MH	Satisfactory Satisfactory	Satisfactory Satisfactory	MH
Typology 2	MH	Banks MSBs VASPs*	ML MH H	MH	Good Good Satisfactory*	Good Good Satisfactory*	MH
Typology 3	ML	Lawyers IB Financing Insolvency Accountants NPOs Real Estate	MH MH L L ML ML ML	MH	Satisfactory Satisfactory Good Good Satisfactory Satisfactory Weak	Satisfactory Satisfactory Good Good Satisfactory Satisfactory Satisfactory	ML
Typology 4	L	Cash* DPMS HVGD	L MH ML	L	Satisfactory Weak Weak	Weak Satisfactory Satisfactory	L

*Weighting greater as per narrative.

The overall residual risk rating for each typology was:

[119] Also taking into account the rating of weak for law enforcement which is applicable to all typologies.

Typology 1 - MH

Typology 2 - MH

Typology 3 - ML

Typology 4 - L

7. Consequences

In the TF context, consequence refers to the impact or harm that a TF threat may cause if eventuated. This includes the effect of the underlying terrorist activity on domestic or institutional financial systems and institutions, as well as the economy and society more generally. Notably, consequences of TF are likely to be more severe than for ML or other types of financial crime (e.g. tax fraud etc.), which impacts how countries respond to identified threats. Consequences of TF are also likely to differ between countries and between TF channels or sources, and may relate to specific communities or populations, the business environment, or national interests. Given the challenges in assessing consequences, countries need not take a scientific approach when considering consequences and instead may want to start with the presumption that consequences of TF will be severe (whether domestic or elsewhere) and consider whether there are any factors that would alter that conclusion.[120]

The WG agreed at its first meeting that this would be the approach whereby there will be a presumption that the consequences are severe, and consideration would be given as to whether this conclusion is altered based on the findings of the assessment.

8. Conclusion

The WG concluded that the risk of the collection of funds for TF in the VI was Low. The risk of the use of funds for TF purposes in the VI was also Low. The risk of funds being moved directly or indirectly through or via the VI was Medium-High. Given the fact that the VI is an international financial and international financial centre, the risk of movement was given a greater weighting, leading to an overall risk rating of Medium-High.

It was identified that the risk to the VI in relation to TF via is the misuse of VI legal entities is Medium-High. Secondly, the risk that the VI entities are used to facilitate the transfer of funds intended to be used for terrorism purposes abroad, particularly with funds/VAs being sent via

[120] FATF TF Risk Assessment Guidance

VI VASPs was found to be Medium-High. The risk that VI service providers such as TCSPs or lawyers may provide services (knowingly or unknowingly) to entities which are involved in TF is Medium-Low. The risk of the VI facilitating the movement through or from the VI of cash or PMS relevant to TF is Low.

Annex I: Recommendations

1. This Risk Assessment should be updated every three years to ensure that accurate and up-to-date data is considered and that changes in risks are recognised in good time and that appropriate mitigating measures can be taken.[121]

2. In accordance with FATF Standards,[122] the RA should be endorsed at the highest level and widely circulated across both public and private sectors to ensure a high level of the understanding of TF risk across the jurisdiction.

3. Training on the findings of this RA should be provided to the public sector.

4. Outreach should be conducted to the private sector regarding the findings of the RA in order that they may gain a better understanding of TF risk to allow for implementation of more effective controls and increase their ability to detect and prevent and mitigate potential TF activities.

FIA - AIU

5. Strategic analysis on the misuse of cash and cash intensive businesses should be considered.

RVIPF Intelligence Unit

6. RIVPF IU should be provided with training on terrorism, TF and red flags.

[121] The FATF Standards requires countries to maintain an up-to-date assessment of their TF risks. While a risk assessment presents a snapshot in time, an assessment of TF risk should be an ongoing and evolving process Jurisdiction experience highlights the particular benefits of embedding a culture of ongoing risk or threat assessment, having ongoing mechanisms to collect relevant information on TF risk, and conducting more targeted TF risk assessments which allow for enhanced stakeholder engagement.

[122] (Jurisdictions should ensure that the findings of the TF risk assessment are endorsed by senior officials, and that all key stakeholders have a common understanding of the outcomes and the relative measures of risk - FATF TF Risk Assessment Guidance, Part 5.

7. RVIPF IU should continue with plans to collect intelligence relating to transfers of funds via informal means, crypto currencies and the movement of goods (in conjunction with HMC).

RVIPF-FCU

8. Recruitment within the RVIPF-FCU of additional resources sufficiently skilled in the area of TF should be completed swiftly and additional resources that have been budgeted for implemented as soon as possible including training of investigators and IT resources particularly in the area of the investigation of VAs.

9. The national strategy on investigations and prosecution of TF should be finalised and include all relevant agencies namely ODPP, FCU, RVIPF Intelligence, HMC, DOI and FIA-AIU as well as the regulators and relevant committees such as CLEA.

10. International Cooperation LEA partnerships with regional and international enforcement agencies should continue to be enhanced.

11. The FCU should continue to collect and consolidate information regarding TF risks and trends and provide updates at CLEA. Outcomes should be monitored.

HMC

12. HMC should ensure that TF Risk is considered in the work being undertaken particularly regarding the cross-border movement of cash and goods, this could potentially be combined with the envisaged creation of a RA Unit and that HMC has sufficient staff to monitor the movement of cross-border cash and goods for TF risk.

13. HMC training should be conducted in relation to the identification of TF in areas such as the movement of goods and precious metals.

14. HMC should enhance the collection of information regarding the movement of PMS and monitor movement in and out of the territory.

CLEA

15. Information sharing and communication should be enhanced bilaterally and committees such as CLEA Collaboration should be both at the strategic level as well as on individual matters at the operational level.

FIA-SEU

16. The FIA-SEU should ensure that DNFBPs it supervises conduct TF specific institutional RA to ensure that they have the relevant and adequate measure in place to mitigate any TF risk and more TF training be provided to management and staff.

17. Employees of the FIA-SEU should undertake TF training.

18. The FIA-SEU should provide targeted TFS outreach and guidance to the DNFBP sector, as well as conduct ongoing targeted TFS offsite and onsite examinations/inspections for the DNFBP sector.

DOI

19. The DOI should enhance its data collection processes to facilitate more detailed demographic analysis and ensure better tracking of immigration trends. These measures will support proactive monitoring and contribute to a more comprehensive RA.

20. DOI training should be conducted in identifying and responding to potential TF threats**.**

FIA AIU

21. The FIA AIU and FIA-SEU should collaborate to conduct strategic analysis reports on TF trends and typologies for the DNFBP sector.

22. The FIA AIU should assess its increased capacity in relation to VA TF / TFS analysis, and proceed to ensure additional employees if needed, and ensure that analysts are engaged in ongoing TF updates that are applicable to TF e.g. moving funds through the territory.

FSC

23. All VASP applications should be processed as a matter of urgency and registered VASPs closely monitored in relation to TF and TFS risk. Policing the perimeter activities should continue to ensure that those VASPs whose applications are refused and continue to carry on business or those who commence operations in the VI prior to being registered are appropriately penalised in accordance with the legal requirements.

Private Sector

24. FIs' and DNFBPs' should ensure:

a. Institutional risk assessments fully consider and account for TF risk exposure

b. Staff are sufficiently trained to understand TF and the TF risk posed by their clients and their business activities

c. Adequate verification and ongoing monitoring is conducted to ensure proper understanding of the nature of business and circumstances of clients to be able to identify potential changes that may signal possible TF activity

d. Staff are adequately trained to identify suspicious activities related to TF

Other

25. In relation to LPLAs, the TF WG adopts the recommendations made in the LPLA RA:

a. Implement more detailed and better representative statistics by LEAs to allow VI to more accurately assess the actual risks detected in relation to VI LPLAs. This should include maintaining easily retrievable statistics in relation to the different types of LPLAs featuring in a SAR or investigation, other involved jurisdictions, predicate offences and other features, including for example, the presence of nominee arrangements.

b. Collect more data relating to LPLAs, including but not limited to nature of business (particularly business that is considered high risk for ML, TF and PF), extent of nominee shareholder arrangements and more detailed information on the use of introducers (for example, the nature of business of introducers and risk level assigned to the introducer).

c. Identify and consider the risks of foreign legal arrangements that have sufficient links to the VI.

d. Ensure that all the elements of FATF Recommendations 24 and 25 are covered within VI legislation and implemented, particularly those relating to the collection and maintenance of accurate and up to date BO information.

e. Once the BO registry for legal persons is established, ROCA should implement a risk-based programme to verify the accuracy of the information in the registry.

f. Once the BO registry is established, the ROCA should implement effective and dissuasive penalties for non-compliance with filing obligations, including false, incomplete or inaccurate filings.

g. ROCA should ensure that all shareholder nominee arrangements for legal persons are registered in the corporate registry and impose penalties for non-compliance with this requirement.

h. Improve compliance with AML/CFT/CPF requirements particularly for the legal and accounting professions through increased outreach, onsite inspections and sanctions for non-compliance, leading to increased compliance by entities, as evidenced in onsite inspections.

i. Provide outreach to the regulated sector, primarily TCSPs, and legal and accounting professionals, on the risks relating to LPLAs in the VI and their role in mitigating that risk.

j. Continue to develop and enhance understanding of risk of LPLAs through typologies and other means and sharing this information with the private sector on a regular basis through Joint Anti-Money Laundering and Terrorist Financing Advisory Committee (**JALTFAC**), newsletter, outreach sessions and other fora.

k. Regulators and LEAs to receive training on how VI LPLAS can be misused to commit the offences of ML, TF and PF. [123]

26. In relation to NPOs the TF WG adopts the recommendations made in the NPO RA:

[123] It must be acknowledged that VI has already started implementing stronger controls in relation to the risk posed by BVIBCs. In September 2024, amendments to legislation were passed in the House of Assembly that require legal persons to provide BO information to the ROCA and ensure this information is kept up to date. This is in addition to the existing requirement to provide such information to their registered agent, which must be a licenced TCSP. These requirements came into force on January 2, 2025, and are in the process of being fully adopted. This new requirement to provide BO information to the ROCA. requires disclosure of corporate directors and nominee shareholders and imposes stronger recordkeeping measures on trusts. These measures, along with continued surveillance, guidance and outreach to the regulated sector to assist them with strengthening their compliance program will result in a reduced risk exposure for the VI once those improvements have been fully implemented.

a. The VI should take steps to promote focused, proportionate and risk-based oversight or monitoring of NPOs.

b. Effective monitoring and supervision of higher risk NPOs should occur as well as developing the SOP for the CFT supervision of NPOs and undertaking periodic outreach and providing guidance.

c. The NPO Board should update its manual system to ensure that information on NPOs is kept up to date, accurate and readily available upon request, particularly for investigative purposes and to facilitate international requests.

d. Outreach to the Banking Sector as it pertains to TF risk to facilitate financial inclusion and reduce the occurrence of derisking within the NPO sector should be conducted.

e. The NPO Board, the FIA and the FSC should implement procedures to facilitate effective sharing amongst each other in relation to registered and incorporated NPOs that are being struck off the register, dissolved, deregistered, sanctioned, or have changed their directors/BOs or structure.

Annex II – Acronyms

List of Acronyms

AGC	Attorney General's Chambers
AI	Artificial Intelligence
AIM	Alternative Investment Market
AIU	Analysis and Investigation Unit
AML	Anti-Money Laundering
AMLRs	Anti-Money Laundering Regulations, 2020 (as amended)
AMLTFCOP	Anti-Money Laundering and Terrorist Financing Code of Practice.
ASD	Authorisation and Supervision Division
AU	Authorisation Unit
BNI	Bearer Negotiable Instruments
BO	Beneficial Owner/Ownership
BTCA	Banks and Trust Companies Act, 2020 (as amended)
BVI	British Virgin Islands
BVIBC	British Virgin Islands Business Company
CARTAC	Caribbean Regional Technical Assistance Centre
CDD	Customer Due Diligence
CFATF	Caribbean Financial Action Task Force
CFT	Countering the Financing of Terrorism
CLEA	Collaborative Law Enforcement Agencies
CMA	Company Management Act, 2020 (as amended)
CPF	Countering Proliferation Financing
CSPs	Corporate Services Providers
DeFi	Decentralised Finance
DLT	Distributed Ledger Technology
DNFBP	Designated Non-Financial Businesses and Professions
DOI	Department of Immigration
DPMS	Dealers in Precious Metals and Stones
DPRK	Democratic People's Republic of Korea
ECDD	Enhanced Customer Due Diligence
EDD	Enforcement Division
EDD	Enhanced Due Diligence
Eis	Eligible Introducers
FATF	Financial Action Task Force
FB	Financing Business
FCDO	Foreign, Commonwealth and Development Office
FCU	Financial Crime Unit
FI	Financial Institution
FIA	Financial Investigation Agency
FIA-AIU	Financial Investigation Agency - Analysis and Investigation Unit
FIA-SEU	Financial Investigation Agency - Supervision & Enforcement Unit
FinCEN	Financial Crimes Enforcement Network
FINTRAC	Financial Transactions & Reports Analysis Centre

FMSA	Financing and Money Services Act, 2020 (as amended)
FSC	Financial Services Commission
GDP	Gross Domestic Product
GO	Governor's Office
GTI	Global Terrorism Index
HMC	His Majesty's Customs
HMG	His Majesty's Government
HVGD	High-Value Goods Dealers
IB	Investment Business
IC	International Cooperation
ICIJ	International Consortium of Investigative Journalists
ICO	Initial Coin Offering
ICT	International Cooperation Team
IFC	International Financial Centre
IMF	International Monetary Fund
INTERPOL	International Criminal Police Organisation
IP	Insolvency Practitioner
IU	Intelligence Unit
JALTFAC	Joint Anti-Money Laundering and Terrorist Financing Advisory Committee
JSC	Joint Supervisory Committee
LEA	Law Enforcement Agency
LPLA	Legal Persons and Legal Arrangements
LPAWG	Legal Persons and Arrangements Working Group
LPLA RA	Legal Persons and Legal Arrangements Risk Assessment
MER	Mutual Evaluation Report
MH	Medium High
ML	Medium Low/ Money Laundering
MLA	Mutual Legal Assistance
MLRA	Money Laundering Risk Assessment
MLRO	Money Laundering Reporting Officer
MOU	Memorandum of Understanding
MSB	Money Services Business
NAMLCC	National AML/CFT Coordinating Council
NCA	National Crime Agency
NFT	Non-Fungible Token
NPO	Non-Profit Organisation
ODPP	Office of the Director of Public Prosecutions
OFAC	Office of Foreign Assets Control
OTC	Over-the-counter trading
OTRCIS	Overseas Territories Regional Crime Intelligence System
PEP	Politically Exposed Person
PF	Proliferation Financing
PIJ	Palestine Islamic Jihad
PMS	Precious Metals and Stones
PSU	Prudential Supervision Unit
PTCs	Private Trust Companies

RA	Risk Assessment
REAs	Real Estate Agents
ROCA	Registrar of Corporate Affairs
RUF	Revolutionary United Front
RVIPF	Royal Virgin Islands Police Force
SAR	Suspicious Activity Report
SEU	Supervisory and Enforcement Unit
SIBL	Securities and Investment Business Act, 2020 (as amended)
SOP	Standard Operating Procedures
SOS	Supervising Oversight System
SSU	Specialised Supervision Unit
TCSP	Trust and Corporate Service Provider
TOR	Terms of Reference
TF	Terrorist Financing
TFRA	Terrorist Financing Risk Assessment
TFS	Targeted Financial Sanctions
TSPs	Trust Services Providers
UAE	United Arab Emirates
UK	United Kingdom
UN	United Nations
USA	United States of America
USD	United States Dollar
USVI	United States Virgin Islands
USVIPD MIT	United States Virgin Islands Police Department Major Incident Team
VAs	Virtual Assets
VASP	Virtual Assets Service Provider
VASPA	Virtual Assets Service Providers Act, 2022
VI	Virgin Islands
WG	Working Group