Money Laundering, Terrorist and Proliferation Financing and Targeted Financial Sanctions

Malta's National Risk Assessment 2023

National Coordinating Committee on Combating Money Laundering and Funding of Terrorism

December 2023

Table of Contents

List of figures

List of tables

1 Foreword

Malta carried out the previous edition of the National Risk Assessment (NRA) on Money Laundering (ML) and Funding for Terrorism (TF) in 2018. From that milestone, Malta addressed the exigencies of reviews by the Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism (MONEYVAL), the European Banking Authority (EBA), the European Commission, and the International Monetary Fund.

In 2019, the fifth round Mutual Evaluation Report (MER) for Malta was published by MONEYVAL that presented several shortcomings. In order to address the recommendations from this report, the focus by Malta has been on having in place a sustainable, risk-based, proactive, responsive, and effective anti-money laundering and countering the funding for terrorism (AML/CFT) framework. Following the publication of the said report, the Maltese government and its national competent authorities embarked on various initiatives to address the recommendations made by MONEYVAL. Malta entered into two separate procedures, one under MONEYVAL to assess the technical matters, and the other with the Financial Action Task Force (FATF), to address the recommendations on effectiveness.

Under MONEYVAL's remit, Malta entered into what is referred to as the enhanced follow-up procedure in which it had to report to MONEYVAL the progress achieved in addressing the recommendations made in the report, particularly those of a technical nature. Under this procedure, MONEYVAL in April 2021, re-rated Malta's compliance with the technical standards, bringing Malta's AML/CFT framework in technical compliance with the FATF recommendations. In this re-rating against the FATF recommendations, Malta achieved a 'largely compliant' or 'compliant' rating for all the recommendations, thus having a robust AML/CFT regime. This led to Malta being one of the two countries under MONEYVAL as the FATF-Style Regional Body that has none of its technical recommendations rated as 'partially compliant'.

Under FATF, Malta entered into the so-called observation period and was expected to report to FATF on the progress it achieved on addressing the recommendations related to effectiveness in respect of which Malta had achieved a 'low' or 'moderate' level of effectiveness in the 2019 MONEYVAL report. Following the observation period, in June 2021[1], the FATF concluded that Malta: "*made progress on a number of the MER's recommended actions to improve its system, such as: strengthening the risk-based approach to FI and DNFBP*[2] *supervision; improving the analytical process for financial intelligence; resourcing the police and empowering prosecutors to investigate and charge complex money laundering in line with Malta's risk profile; introducing a national confiscation policy as well as passing a non-conviction based confiscation law; raising sanctions available for the crime of TF and capability to investigate cross-border cash movements for potential TF activity; and increasing outreach and immediate communication to reporting*

[1] https://www.fatf-gafi.org/content/fatf-gafi/en/publications/High-risk-and-other-monitored-jurisdictions/Increased-monitoring-june-2021.html#malta

[2] Under the FATF Glossary, *designated non-financial businesses and professions* (DNFBPs) means a) Casinos; b) Real estate agents; c) Dealers in precious metals; d) Dealers in precious stones; e) Lawyers, notaries, other independent legal professionals and accountants; and f) Trust and Company Service Providers. FATF Glossary (fatf-gafi.org)

entities on targeted financial sanctions and improving the TF risk understanding of the NPO sector."

Nevertheless, the FATF also concluded that further improvements were needed with regard to two areas under the effectiveness outcomes. These were in relation to the accuracy of beneficial ownership information and related sanctioning where breaches are identified, and to the use of financial intelligence, specifically in pursuing criminal tax and related ML cases. As a result of these, Malta was placed under the list of jurisdictions under enhanced monitoring (also commonly known as the 'grey-list') in June 2021.

During the period from June 2021 and June 2022 (a span of twelve months), as reported by FATF[3], *'the FATF welcomes Malta's significant progress in improving its AML/CFT regime. Malta has strengthened the effectiveness of its AML/CFT regime to meet the commitments in its action plan regarding the strategic deficiencies that the FATF identified in June 2021 related to the detection of inaccurate company ownership information and sanctions on gatekeepers who fail to obtain accurate beneficial ownership information, as well as the pursuit of tax-based money laundering cases utilising financial intelligence. Malta is therefore no longer subject to the FATF's increased monitoring process. Malta should continue to work with MONEYVAL to sustain its improvements in its AML/CFT system.'* This led to Malta being removed from FATF increased monitoring in record time.

Malta's strategy in addressing the FATF action plan was based on three important policy considerations: enhanced risk understanding; effective delivery; and sustainability.

During Malta's so-called grey-listing period, an enhanced understanding of risk has been achieved through the carrying of two thematic risk assessments. One of these risk assessments was on assessing the risk of concealment of beneficial ownership, and another on assessing the ML risks associated with tax crimes. This improved risk understanding, accompanied by risk-based supervision and enforcement in relation to beneficial ownership, and criminal investigations and prosecutions in relation to tax-related ML, were key to ensure effective delivery, which was also acknowledged by the FATF, and Malta's subsequent removal from the so-called grey-list.

The 2023 NRA continues to build on what has been achieved thus far, to ensure that all stakeholders continue to have a solid understanding of the ML/TF risks that Malta and its sectors and operators are exposed to, and to ensure that the AML/CFT framework is dynamic and proactive and responds appropriately to any ML/TF risks or gaps.

This NRA was launched in March 2021, with the full support of the Minister for Finance and Employment, and under the coordination of the Malta's National Coordinating Committee on Combating Money Laundering and Funding of Terrorism (NCC). As explained in further detail in section 6, all relevant authorities in Malta actively contributed to enhancing Malta's ML/TF risk understanding and participated in this iteration of the NRA. Furthermore, the assistance of renowned AML/CFT consultant, Mr Yehuda Shaffer, was also sought to further strengthen Malta's 2023 NRA.

[3] https://www.fatf-gafi.org/en/publications/High-risk-and-other-monitored-jurisdictions/Increased-monitoring-june-2022.html#Malta

The process of the updating Malta's NRA entailed extensive policy deliberations and strong inter-institutional and stakeholder dialogue, including with private sector representatives, decisions on further institutional and stakeholder strengthening, and sheer hard work despite several challenges, including COVID-19 external challenges that impacted as well on the findings, as it led to changes in the *modus operandi* of financial crime.

All this could not have materialised without the right motivation and a strong ownership by all stakeholders and unrelenting political commitment and support. Only through this holistic and national approach can the NRA address the objective of enhancing the risk-based approach adopted by Malta's supervisory and law enforcement authorities and the private sector, and ensuring that it would serve our country well, not only in the foreseeable future but over the longer-term through regular monitoring and updating. This NRA will continue to ensure that the progress Malta achieved thus far is maintained, and that Malta is well-attuned to meet current and future challenges.

2 Executive summary

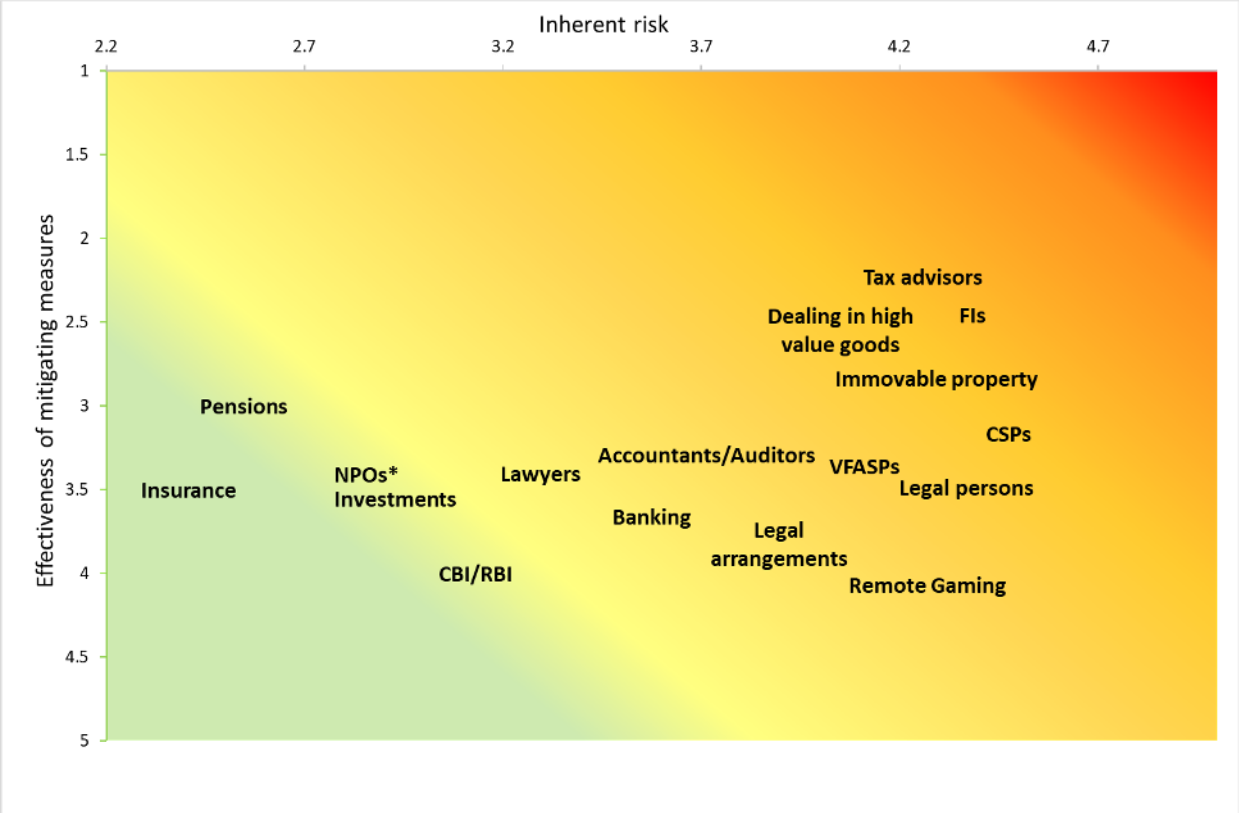
The 2023 NRA is the latest iteration of the process by Malta that seeks to identify threats and vulnerabilities in ML, TF, as well as for the first time, proliferation financing (PF) and targeted financial sanction (TFS) related risks. The purpose of the NRA is two-fold:

(i) to establish a common understanding among competent authorities, including supervisory authorities and law enforcement authorities, of the risks of ML, TF, PF and TFS, thereby improving and ensuring that risk-based mitigation measures are implemented nationally; and
(ii) to ensure a strong risk understanding in the private sector with a view to enhancing the risk-based approach and alignment with the priorities, risks and recommendations identified in the NRA.

The methodology adopted was that of assessing the threats, and the vulnerabilities by analysing the likelihood and the impact, and the likelihood and exposure respectively, and the mitigating measures in place, to thereafter derive the residual risk. The analysis took also into consideration the approach adopted in the European Union Supranational Risk Assessment (EU SNRA), the recommendations in the 2019 Mutual Evaluation Report for Malta, the Post-Observation Period Report for Malta, and the reports by the EBA, FIAU strategic analysis and but above all, focused on constructive discussions with set-up working groups and discussions with the private sector representatives. The objective of the 2023 NRA was to gain from these discussions and from the analysis of data from several sources, a sufficiently granular appreciation of the actual threats and vulnerabilities faced by these sectors.

The following figure shows the results of the ML sectoral residual risks in the form of a heat map, showing the inherent risk on the horizontal axis and the effectiveness of mitigating measures on the vertical axis. This map provides only a generalised graphic representation of the ML risk in Malta and does not indicate, at a detailed level, the specific levels of types of risk that exist for a specific sector. To arrive at such a detailed analysis, the sections that follow need to be referred to accordingly.

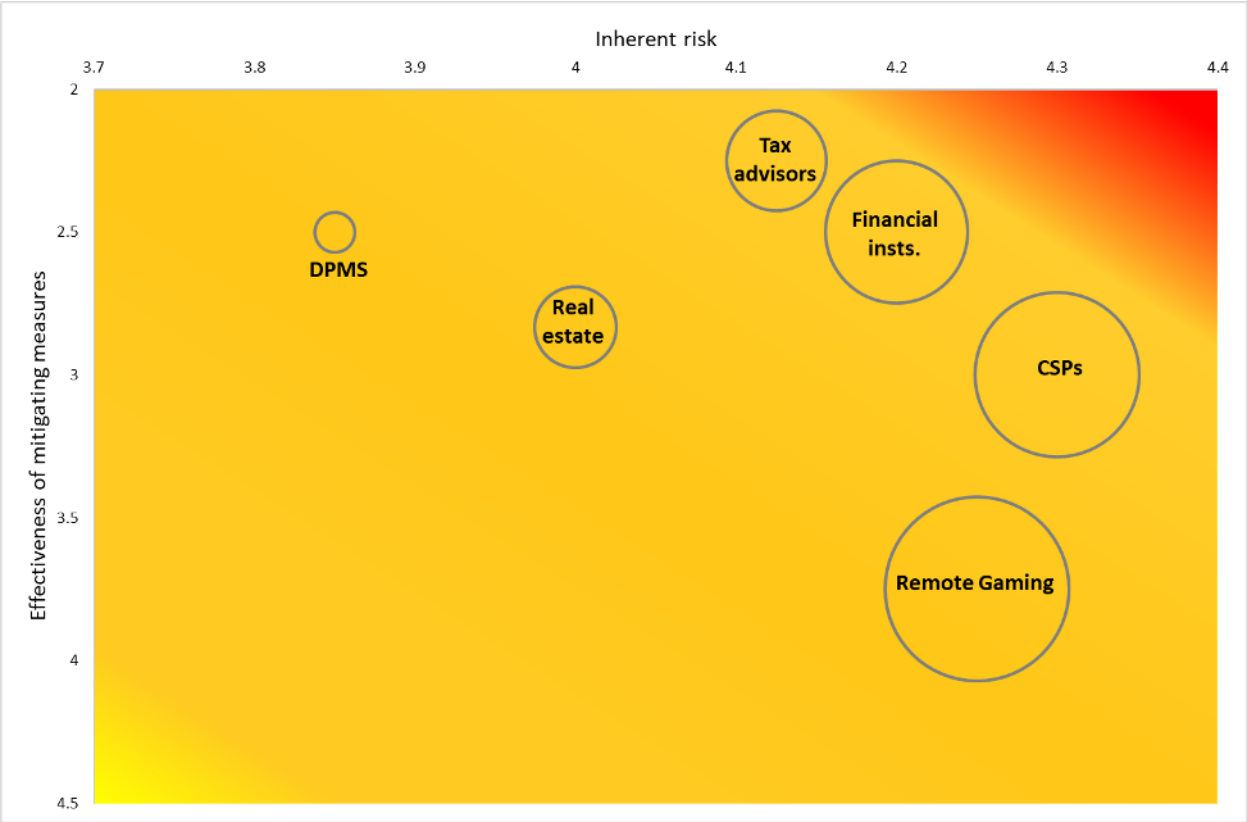
Figure 1: Money Laundering sectoral residual risk heat map



**Non-profit organisations (voluntary organisations)*

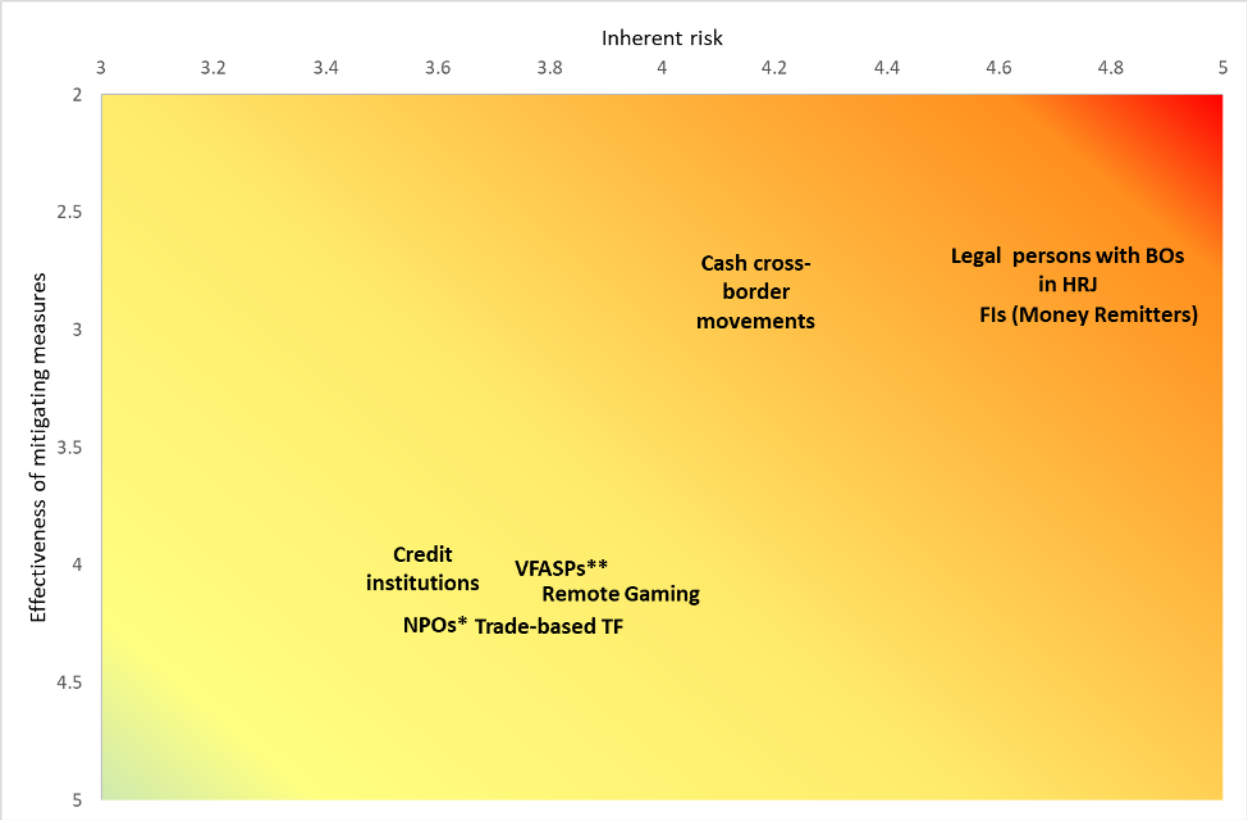
The most material sectors amongst those which scored a 'medium-high' score are presented in the following figure. This figure presents a heat map where the size of the bubble is determined by the materiality of the sector, that takes into consideration the size of the sector, in terms of the assets held, the value of the transactions, and the turnover recorded (on the basis of findings presented in Section 8.3 of this document).

Figure 2: Sector materiality (based on assets held, value of the transactions processed, turnover, percentage share of the total GDP, and number of clients) of higher risk sectors



The following figure shows the results of the TF residual risk in the form of a heat map, showing the inherent risk on the horizontal axis and the effectiveness of mitigating measures on the vertical axis. Similar to the ML residual risk heat map, this map provides only a generalised graphic representation of the TF risk in Malta and does not indicate, at a detailed level, the specific levels of types of risk that exist for a specific sector. Such detailed analysis is presented in section 12 of this document.

Figure 3: Terror Financing residual risk heat map[4]

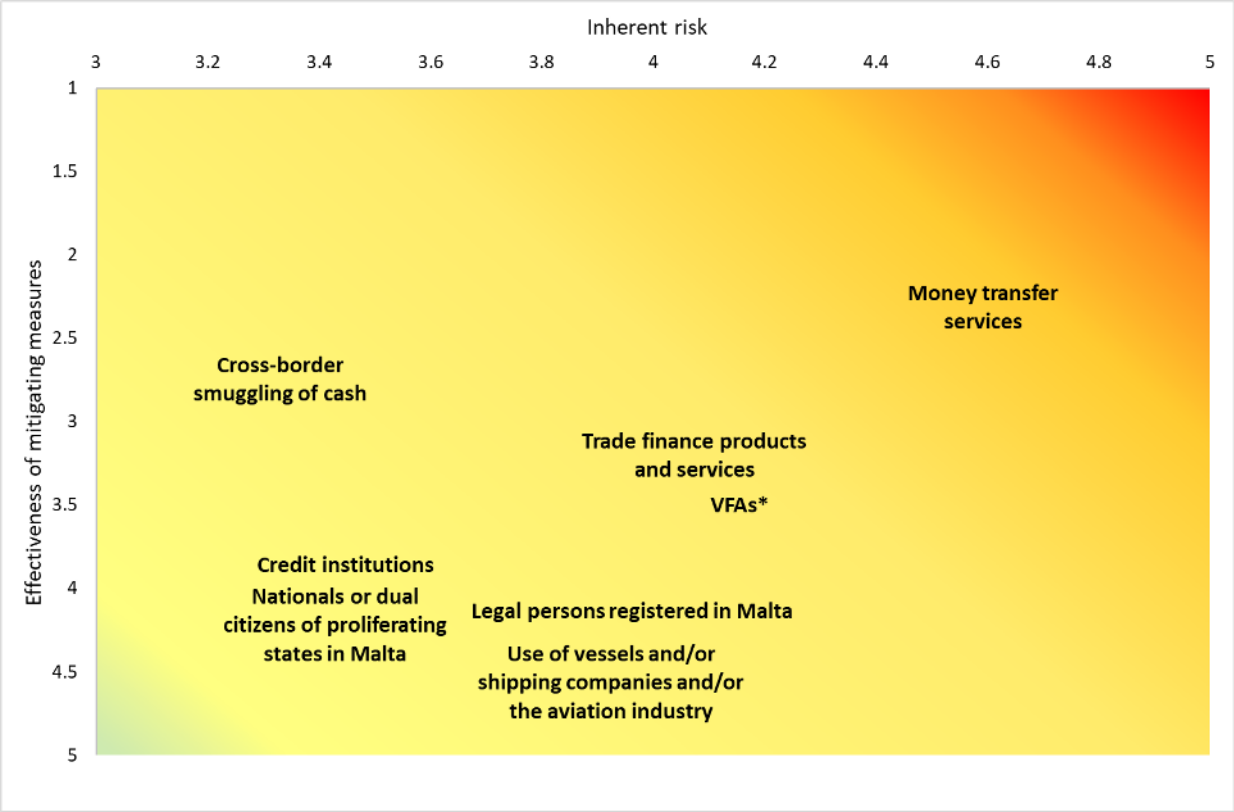


**Non-profit organisations (voluntary organisations)*
***This refers to the licensed VFASPs. For the residual risk in relation to the crypto assets reference is to be made to section 10.3.*

The following figure shows the results of the PF and TFS residual risks in the form of a heat map, showing the inherent risk on the horizontal axis and the effectiveness of mitigating measures on the vertical axis. Similar to the previous heat maps, this map provides only a generalised graphic representation of the PF and TFS risks in Malta and does not indicate, at a detailed level, the specific levels of types of risk that exist for a specific sector. Such detailed analysis is provided in section 13 of this document.

[4] Sectors not mentioned in this heat map should apply *mutatis mutandis* risk level as in ML.

Figure 4: Proliferation Financing and Targeted Financial Sanctions residual risk heat map



**This refers to the licensed VFASPs. For the residual risk in relation to the crypto assets reference is to be made to section 10.3.*

The following table summarises the NRA results for 2018 and 2023. As can be seen, a decline in the residual risk has been identified across most sectors, and this should be attributed mostly to the improvement of mitigating measures applied.

The table by itself is not a substitute to a full understanding of the risks and their mitigation measures as described in full detail in this iteration of the NRA, that also presents applicable recommendations in view of the risks presented for the subject persons.

Table 1: 2018 NRA results vs 2023 NRA results

Risk assessment	2018 NRA residual risk	2023 NRA residual risk
Money Laundering – residual risk		
Financial sector		
Banking	Medium-high	Medium
Financial Institution	Medium-high	Medium-high
Investment services	Medium-high	Medium
Pensions	Medium	Medium
Insurance	Medium	Medium-low
DNFBPs		
Gaming		
Remote gaming	High	Medium
Land-based gaming	Medium-low	Medium
Recognition notice framework	N/A	Medium-high
CSPs	High	Medium-high
Accountants and auditors	Medium-high	Medium
Lawyers	High	Medium
Tax advisors	N/A	Medium-high
Dealing in immovable property	Medium-high	Medium-high
High value goods	N/A	Medium-high
VFAs and VFASPs*		Medium
Other instruments - ML residual risk		
Legal persons	High	Medium-high
Legal arrangements	High	Medium
Citizenship & residency by investment schemes	N/A	Medium
NPOs (Voluntary Organisations)	High	Medium
Terrorism Financing**		Medium
Proliferation Financing and Targeted Financial Sanctions related risks	N/A	Medium

*The VFA sectoral ML/TF risk assessment was carried out in October 2019 and given Malta's control environment that was developing rapidly and given that at the time of writing Malta was at the forefront of international efforts to supervise and regulate this sector, a typical controls assessment approach and subsequent analysis of residual risk was avoided.

**No overall residual risk rating was provided in the 2019 TF risk assessment.

Note: N/A implies not applicable during the period under consideration.

3 Introduction

The 2023 NRA is the latest iteration of the process by Malta that seeks to identify threats and vulnerabilities in ML, TF, as well as for the first time, PF and TFS related risks. The purpose of the NRA is two-fold: (i) to establish a common understanding of the risks involved in the field of ML, TF, and PF and TFS related risks for the competent authorities[5] (that includes the supervisory authorities[6]) and law enforcement authority and thereby improve mitigation measures through an enhanced risk-based approach; and (ii) for the benefit of the private sector, particularly with regard to enhancing their risk-based approach with the priorities identified.

The layout of this publication is as follows: primarily an overview of the previous ML/TF related risk assessments carried out in Malta is presented followed by how the EU Supranational Risk Assessment is taken into consideration throughout the whole NRA process. This is followed by a section on the stakeholders and the methodology adopted, as well as a section outlining the contextual factors of Malta. Further to this an analysis, a section presenting the results of the 'non-financial product' follows with a focus on legal persons, legal arrangements, citizenship and residency by investment schemes, and voluntary organisations. The results of the main threats of laundering foreign and domestic proceeds of crime in Malta follows, with the results of the financial sector and the designated non-financial businesses and professions (DNFBPs) presented primarily. The financial sector part presents the results by sector and product focusing on the banks, the financial institutions, investment securities, insurance, and pensions. The DNFBPs include the analysis on lawyers, accountants, lawyers, and tax advisors and the company service providers (CSPs), the immovable property, real estate agents and the notaries, the high value goods sector, and the gaming sector. This is followed by a section on Virtual Financial Assets (VFAs) and Virtual Financial Asser Service Providers (VFASPs), followed by the overall ML risk section.

Thereafter, the focus is on presenting the results of the TF risks from the raising, moving and use of funds. Subsequently, the results of the PF and TFS related risks are presented. This is the first time that Malta carries out this risk assessment on PF in line with the October 2020 revision by the

[5] In line with the subsidiary legislation 373.01 of the Prevention of Money Laundering and Funding of Terrorism Regulations (2018), 'competent authority' means: *any supervisory authority, the Comptroller of Customs when carrying out duties under any regulation that may be issued or are in force from time to time relating to the cross-border movement of cash and other financial instruments, the Commissioner for Revenue, the Commissioner for Voluntary Organisations, the Asset Recovery Bureau, the Security Service; and, the Sanctions Monitoring Board.* https://legislation.mt/eli/sl/373.1/eng/pdf

[6] Subsidiary Legislation 373.01 of the Prevention of Money Laundering and Funding of Terrorism Regulations explains that 'supervisory authority' includes *(a) the Central Bank of Malta; (b)the Malta Financial Services Authority; (c) the Registrar of Companies acting under articles 403 to 423 of the Companies Act; (e) an inspector appointed under article 30 of the Insurance Business Act, including when such inspector exercises his functions for the purposes of the Insurance Intermediaries Act by virtue of article 54 thereof; (f) a person appointed under article 20 or article 22 of the Banking Act; (g) a person appointed under article 14 or article 15 of the Financial Institutions Act; (h) a person appointed under article 13 or article 14 of the Investment Services Act; (i) the Lotteries and Gaming Authority acting under the Lotteries and Other Games Act and the Gaming Act, and any regulations issued thereunder; (j) a person appointed under article 17 of the Lotteries Cap. 438. and Other Games Act; (k)the Comptroller of Customs when carrying out duties under any regulations that may be issued or are in force from time to time relating to the cross-border movement of cash and other financial instruments; (l) the Quality Assurance Oversight Committee appointed by the Accountancy Board under the Accountancy Profession Act.* LEĠIŻLAZZJONI MALTA (legislation.mt)

FATF, of Recommendation 1 and its Interpretative Note requiring countries to assess their potential breaches, non-implementation or evasion risks relating to proliferation financing referred to under FATF Recommendation 7.[7] A summary table is presented in the concluding part highlighting the residual risk rating of the products and sectors analysed in the iteration of this NRA.

Each section presents specific recommendations that highlight the salient points that subject persons are to encompass in their day-to-day activities for an enhanced risk-based activity and to ensure a sustainable, risk-based, proactive, responsive and effective AML/CFT framework.

It is to be noted, that this publication is backed by detailed restricted working papers which include both additional data and analysis. Explanatory text in this publication reflects only partially the analysis carried out in the working papers, wherein this publication, the focus is mostly on the topics that have a 'high' or 'medium-high' rating.

Subject persons are to assess their risks not only based on the analysis in their respective sectoral section of the 2023 NRA, but also on additional sections, such as, the overall ML risks 'section 11', 'section 12' that presents the TF risks, 'section 13' on PF and TFS related risks, as well as the other relevant other instruments in 'section 9'.

4 2018 National Risk Assessment and other sectoral risk assessments

Malta carried out the previous NRA in 2018[8]. In the interim between 2018 and the process for an updated NRA, Malta carried out a series of sector-specific risk assessments. These include risk assessments focusing on (i) virtual financial assets (VFAs); (ii) TF; (iii) organised crime; (iv) use of cash and the shadow economy; (v) corruption; (vi) concealment of beneficial ownership; and (vii) the laundering of the proceeds of tax crimes. All of these contributed to the follow-up process to Malta's mutual evaluation by MONEYVAL in 2019 and to the high-level political commitment to work with the FATF and MONEYVAL that Malta made on the 25 June 2021.

With the launching of the National Anti-Money Laundering/Countering the Funding for Terrorism/Targeted Financial Sanctions (AML/CFT/TFS) Strategy for 2021-2023[9] Malta also committed itself to update the NRA. In fact, under policy goal II of the latter mentioned Strategy the key action is that AML/CFT policies and activities of all authorities will be prioritized and guided by an updated risk assessment focusing on Malta's profile as a financial centre and other risk factors.

The 2018 NRA, the legal persons and legal arrangements and the voluntary organisations (VOs) or the non-profit organisations (NPOs), the Virtual Financial Assets (VFAs), and the TF risk assessments have now been superseded by this NRA which has an overarching role in the analysis of risks and mitigating measures and recommendations that seek to lower the inherent risks posed by products and services that contextualize Malta. The risk assessments on concealment of beneficial ownership, and the risk assessment on the laundering of the proceeds of tax crimes

[7] The FATF Recommendations (fatf-gafi.org)
[8] Result_of_the_NRA_2018.pdf (gov.mt)
[9] National Coordinating Committee (gov.mt)

carried out in 2021 have fed into this iteration of the NRA. In 2021, in order to address the FATF action plan[10], Malta carried out a National Risk Assessment on Money Laundering of the Proceeds of Tax Crime in Malta. This risk assessment identified the drivers behind the money laundering risks in Malta in relation to proceeds of domestic and foreign tax crime and also sought to identify the mitigating measures and applicable recommendations. This assessment was coordinated by the NCC and with intelligence shared from the FIAU, the MTCA, the OAG, the Financial Crimes Investigations Department (FCID), Komunita' Agenzija Malta, the Department of Customs (MTCA) and the Central Bank of Malta. In addition, Malta in August 2021, carried out a risk assessment on the concealment of beneficial ownership with an emphasis on commercial partnerships. This assessment was carried out with the contribution of the MBR, the FIAU, the MFSA, the MTCA, the OAG, representative bodies of the private sector, and coordinated by the NCC. These risk assessments were both acknowledged by FATF in the de-listing process for Malta.

The NRA in the context of this analysis is in line with the requirements of the risk-based approach of FATF recommendation 1 on assessing risks and applying a risk-based approach and take commensurate preventative measures, when stating: '*Countries should identify, assess, and understand the money laundering and terrorist financing risks for the country, and should take action, including designating an authority or mechanism to coordinate actions to assess risks, and apply resources, aimed at ensuring the risks are mitigated effectively. Based on that assessment, countries should apply a risk-based approach (RBA) to ensure that measures to prevent or mitigate money laundering and terrorist financing are commensurate with the risks identified',* and that *'Countries should also identify, assess, and understand the proliferation financing risks for the country.'*[11]

This NRA process is also addressing the requirements of Subsidiary Legislation 373.02[12], article 5(c) that states that the NCC *'shall also conduct any necessary follow-up action to monitor and ascertain the effective implementation of the national strategy and policies and the actions intended to address any threats, vulnerabilities and risks identified following the carrying out of national risk assessments and to keep that risk assessment up to date.'* The NCC will be coordinating the updating of the NRA that is to be aligned to every National AML/CFT/TFS Strategy, that is every three years, in order to ensure that there is a continuously updated risk-based approach by the supervisory and law enforcement authorities.

5 EU Supranational Risk Assessment

As recommended in the European Union (EU)'s 4th Anti-Money Laundering Directive[13], Malta similar to other EU Member States, has to consider the findings of the EU's Supranational Risk Assessment (EU SNRA) in its own considerations and explain how the findings were embedded in the NRA process.

[10] Documents - Financial Action Task Force (FATF) (fatf-gafi.org)
[11] Recommendation 1: Assessing risks and applying a risk-based approach * (cfatf-gafic.org)
[12] https://legislation.mt/eli/sl/373.2/eng/pdf
[13] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015L0849&from=EN

In this NRA process, Malta in its analysis of the products and services, has initiated every analysis by assessing what are the findings from the 2022 EU SNRA[14] and how do these compare, apply and rate within Malta's context.

6 Stakeholders in the NRA

This iteration of the NRA was coordinated by the NCC and has involved both authorities (these include the Financial Intelligence Analysis Unit, Malta Business Registry, Malta Financial Services Authority, Malta Gaming Authority, Malta Police Force, Office of the Attorney General, Asset Recovery Bureau, Commerce Department, Malta Tax and Customs Administration, Central Bank of Malta, Sanctions Monitoring Board, Office of the Commissioner for Voluntary Organizations, Malta Security Service, Transport Malta, Shipping Registry, and the Ministry for Finance and Employment) and the private sector in the form of the representative bodies of the different subject persons. In addition, Malta has contracted the services of a foreign renowned consultant, Mr Yehuda Shaffer, to assist with the NRA process.

The following table presents the competent and law enforcement authorities with a brief description, that were involved in the NRA.

Table 2: Key Ministries/ Departments/Authorities stakeholders in the NRA

National Coordinating Committee on Combating of Money Laundering and Funding of Terrorism (NCC)	Established within the Ministry for Finance and Employment (MFE) through Subsidiary Legislation S.L. 373.02. The NCC is the governing body responsible for the general oversight of AML/CFT policy. It is responsible for promoting effective collaboration between regulators and law enforcement agencies, and for monitoring interaction between them.
Financial Intelligence Analysis Unit (FIAU)	Responsible for the: • collection, collation, processing, analysis and dissemination of information to combat ML and TF. • monitoring and enforcing compliance by Subject Persons with their AML/CFT obligations. • Monitoring compliance with the Use of Cash (Restrictions) Regulations. • Administering the Centralised Bank Account Register. • Provides training, guidance, and outreach.
Malta Financial Services Authority (MFSA)	Regulator for financial services ensuring adequate systems and controls throughout all regulated entities / Manager of the Trust UBO Register – TUBOR.
Malta Gaming Authority (MGA)	Regulator of the various sectors of the gaming industry
Malta Business Registry (MBR)	Regulator for legal entities in Malta, responsible for their registration and legislative compliance.

[14] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52022SC0344&from=EN

	Responsible for the Beneficial Owner (BO) register.
Malta Tax and Customs Administration (MTCA)	Ensures compliance by all persons and entities with Malta's tax legislation.
Office of the Commissioner for Voluntary Organisations (OCVO)	Overseeing and licensing of non-profit and voluntary organisations.
Malta Customs Department	Monitoring the cross-border transportation of cash.
Commerce Department, Trade Licensing Unit	Responsible for licencing the importation, exportation or transhipment of military goods and dual used goods and licensing of dealers in precious metals and stones.
Malta Freeport Terminal	Malta Freeport Corporation/Authority is the regulator of the Malta Freeport. It issues licences to the operator; it is the landlord and is regulated by the Malta freeport act of 1989. Furthermore, it is responsible for the security of the Freeport within the parameters.
Agenzija Komunita Malta (Community Malta Agency)	Responsible for administering all Maltese citizenship-related matters.
Residency Malta Agency (RMA)	The Government entity responsible for managing and promoting Malta's residency-by-investment programme.
Malta Security Service (MSS)	Responsible for the gathering, analysis and dissemination of operational analysis.
Malta Police Force (MPF)	Specifically, the Financial Crimes Investigations Department, the Cybercrime Unit, the Blockchain Analysis Unit, the Immigration, and the anti-Drug Trafficking Unit.
Office of the Attorney General (OAG)	The constitutionally independent prosecution service of the Republic of Malta.
Office of the State Advocate (OSA)	The principal advisor to Government in matters of law and legal opinion.
Court Services Agency (CSA)	Caters for all civil and criminal proceedings.
Asset Recovery Bureau (ARB)	The functions of the Asset Recovery Bureau can be divided into three main categories: - Tracing of assets - Asset Management - Assets Disposal
Transport Malta (TM)	Manages Malta's Shipping registry and responsible for ensuring compliance by shipowners with Malta's laws and international obligations. The land and aviation industry were involved.
Civil Aviation	Oversees aviation operations and licencing.
Central Bank of Malta (CBM)	Oversees Malta's monetary and fiscal policies.
Ministry for Finance and Employment (MFE)	Responsible for the formulation of Malta's macroeconomic policies.
Sanctions Monitoring Board (SMB) - Ministry for Foreign and European Affairs and Trade	Responsible for ensuring the effective implementation of sanctions including proliferation financing. The FIAU/MFSA/MGA cooperate with the SMB in ensuring that subject persons are compliant with orders

	issued under the National Interest Enabling Powers Act (NIA), Regulations of the Council of the EU, and United Nations Security Council Resolutions related to terrorism, financing of terrorism, and financing of proliferation of weapons of mass destruction.
Identity Malta	Responsible for civil registrations, public deed registrations, issuance of passports, residence permits and electronic identity card.
Accountancy Board	Established in 1979 when the Accountancy Profession Act Cap 281 was enacted. The Board regulates the accountancy profession in Malta
Real Estate Licensing Board (RELB)	The role of the Licensing Board, set up in terms of the Real Estate Agents, Property Brokers and Property Consultants Act (Chapter 615 of the laws of Malta), is to regulate players within the real estate and property market in Malta by issuing appropriate licenses to applicants. The Board is also tasked with all matters relative to the provision and validity of such licenses.
National Statistics Office (NSO)	Responsible for the compilation of official statistics.

The private sector input was invaluable particularly in view of their intimate understanding of their own product vulnerability. For this reason, several meetings have been scheduled with the private sector representative bodies to provide direct input into the NRA so as to better calibrate the findings and the final NRA output. Private sector representative bodies involved are shown below:

Table 3: Private sector representative bodies

Malta Bankers' Association	Represents the interests of banks that are licensed to operate in Malta.
VFA agents' forum	Business section dedicated to the Virtual Financial Assets (VFA) Agents operating under the VFA Act, Chapter 590 of the Laws of Malta which came into effect on the 1st of November 2018, was set up within the Malta Chamber of Commerce, Enterprise and Industry.
Institute of Financial Services Practitioners	An association of professionals working across the entire range of financial services.
Malta Asset Service Association	A channel of communication and to make representations to the Maltese Government and the Malta Financial Services Authority on legislative, regulatory and fiscal matters which amongst others, directly or indirectly, have an effect on the business and/or professional interests of its members.
Malta Insurance Association	A non-profit-making organisation that represents the views and common interests of all insurance companies in Malta.
Malta Association of Insurance Brokers	An association of most of the major insurance brokers in Malta.

Financial Institutions Malta Association	Local association representing licence financial institutions in Malta.
Chamber of Small and Medium Sized Enterprises	Malta's national organisation of independent private businesses.
Malta Chamber of Commerce, Enterprise and Industry	Actively represents companies from all economic sectors and ensure that entrepreneurs enjoy the best competitive environment and regulatory conditions possible for the conduct of business.
Used Vehicles Importers Association	Registered as an Employers' Association in terms of the Industrial Relations Act, Chapter 266 of the laws of Malta and represents the main used vehicles importers.
Malta Crafts Foundation	A public organisation, established in 2021, dedicated to enabling the preservation, appreciation and sustainability of Maltese artisanal products and skills.
Malta Maritime Law Association	The MMLA plays a key role in ensuring that the Maltese maritime legislative and regulatory infrastructure is constantly updated, revised, amended and improved in a pro-active and well-researched manner, in order to enhance qualitative standards as well as to further consolidate Malta's pre-eminent position as an international maritime services centre.
Institute of Financial Services Practitioners	An association of professionals working across the entire range of financial services
Malta Institute of Accountancy	Provide professional guidance, technical support and continued professional education to accountants.
Chamber of Advocates	Represents the warranted lawyers admitted to the Bar of Malta
Notarial Council of Malta	The Notarial Council is the official representative body of the Notarial College, composed of nine members, elected by the General Assembly of the Notarial College from among Notaries in the exercise of their profession composing the said College.
Malta Institute of Taxation	An independent and autonomous body made up of, and run by, tax practitioners which works to promote knowledge and good practice in the tax profession.
Malta Developers Association	Brings together the large majority of private real estate developers, estate agents and other interested parties under one single umbrella.
Malta Financial Services Advisory Council (MFSAC)	The MFSAC was formed in 2021 in part to develop the strategy for the financial services sector in Malta.

Apart from the bodies listed above, meetings were also held with individual firms of the representative bodies.

7 Methodology of the NRA

Further to the launching of the NRA in March 2021, a series of meetings were held by the NCC in the first half of 2021 to:

(i) agree and set out the methodology to be followed in the carrying out of the said risk assessment
(ii) agree on the constitution of different Working Groups and their composition; and
(iii) explain to all interested parties their role within the said process.

The methodology adopted is a simplified, Malta specific, version of the World Bank methodology that was used in the 2018 NRA. This methodology took also into consideration the methodology adopted in the EU SNRA, the 2019 Mutual Evaluation Report for Malta, the Post-Observation Progress Report for Malta, FIAU strategic analysis, and the reports by the EBA, but above all, focused on constructive discussions in the different set-up working groups and discussions with the private sector representatives. The objective of the 2023 NRA was to gain from these discussions a sufficiently granular appreciation of the ML/TF threats and vulnerabilities faced by these sectors in Malta. The following figure shows the NRA process.

Figure 5: NRA process

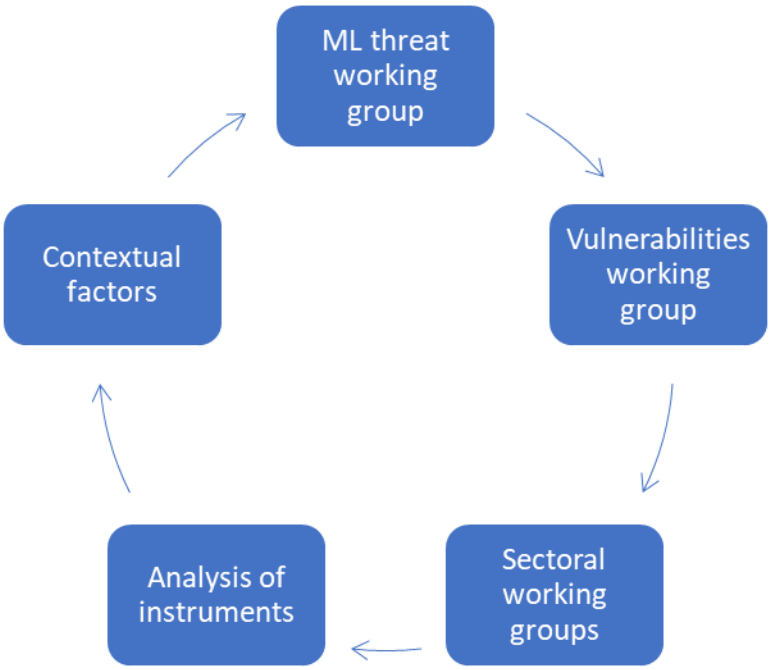


Figure 5 presents the NRA process and illustrates how the sectoral working groups and the analysis of other instruments[15], and the various sectors feeds into the ML threat working group and the vulnerabilities working group.

[15] Refer to section 9 of this NRA for an analysis of 'other instruments'.

There were overall five (5) national working groups as indicated in the table below, that focused on the ML threats, ML vulnerabilities, TF working group and the PF and TFS working group. This table shows the chairperson and the participants of each national working group.

Table 4: National working groups

National working groups	Chairperson	Participants
ML threats	NCC	FIAU, MFSA, MBR, MGA, OCVO, MTCA, SMB, CBM, AG, MPF, ARB, Malta Freeport Terminal, Court Services Agency
ML vulnerabilities	AG	State advocate, FIAU, MFSA, MBR, MGA, OCVO, MTCA, MPF, NCC
TF	MSS	Office of the AG, CBM, FIAU, MPF, MFSA, MBR, SMB, OCVO, MTCA, NCC
PF and TFS	SMB	Office of the AG, CBM, FIAU, MPF, MFSA, MBR, OCVO, MTCA, MSS, NCC

The following figure presents the types of data used in the ML threat working group along with the participants of this working group.

Figure 6: Types of data in the ML threat working group

As indicated in figure 5, the subsequent step involved the vulnerabilities working group. The process in this working group was as follows:

Figure 7: Vulnerability working group process

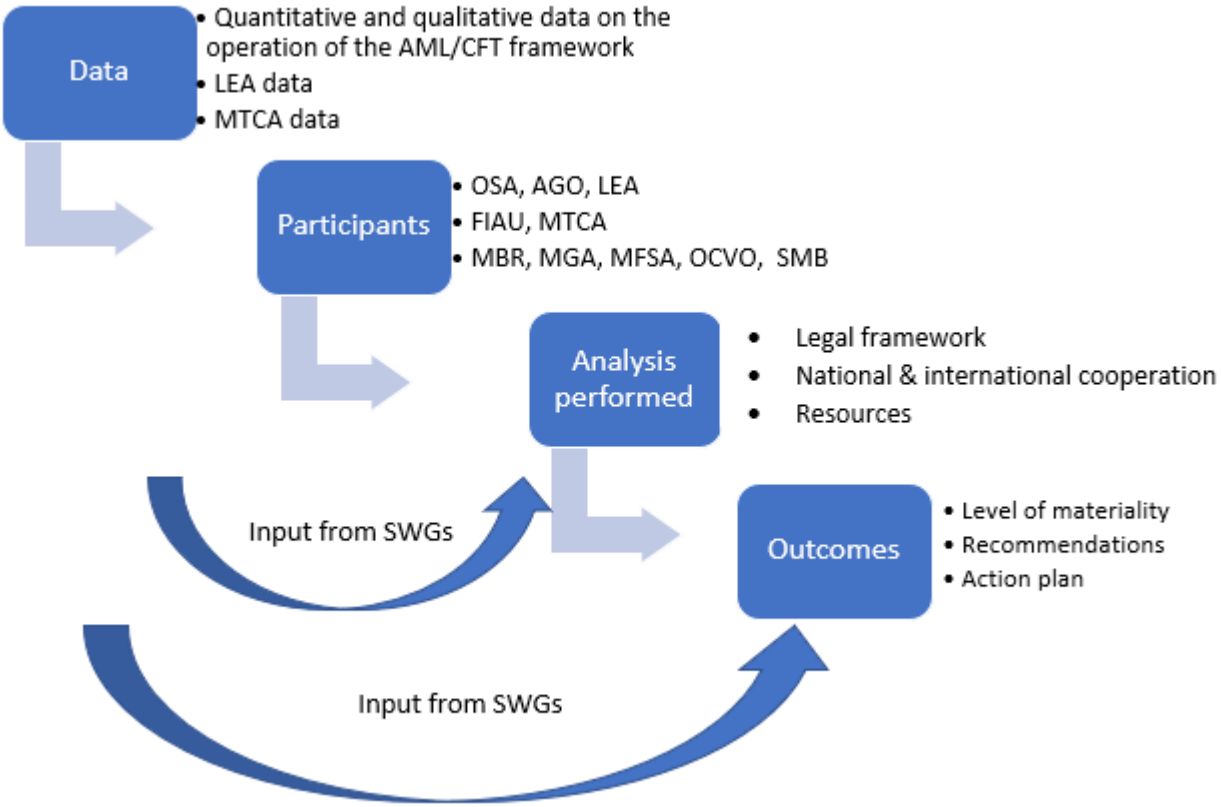


Figure 7 presents the data sources in the vulnerability working group, the participants, the analysis performed, and the outcomes from this working group. It also presents the stages where the input from the sectoral working groups (SWGs) fed into the analysis and the outcomes of the vulnerability working group.

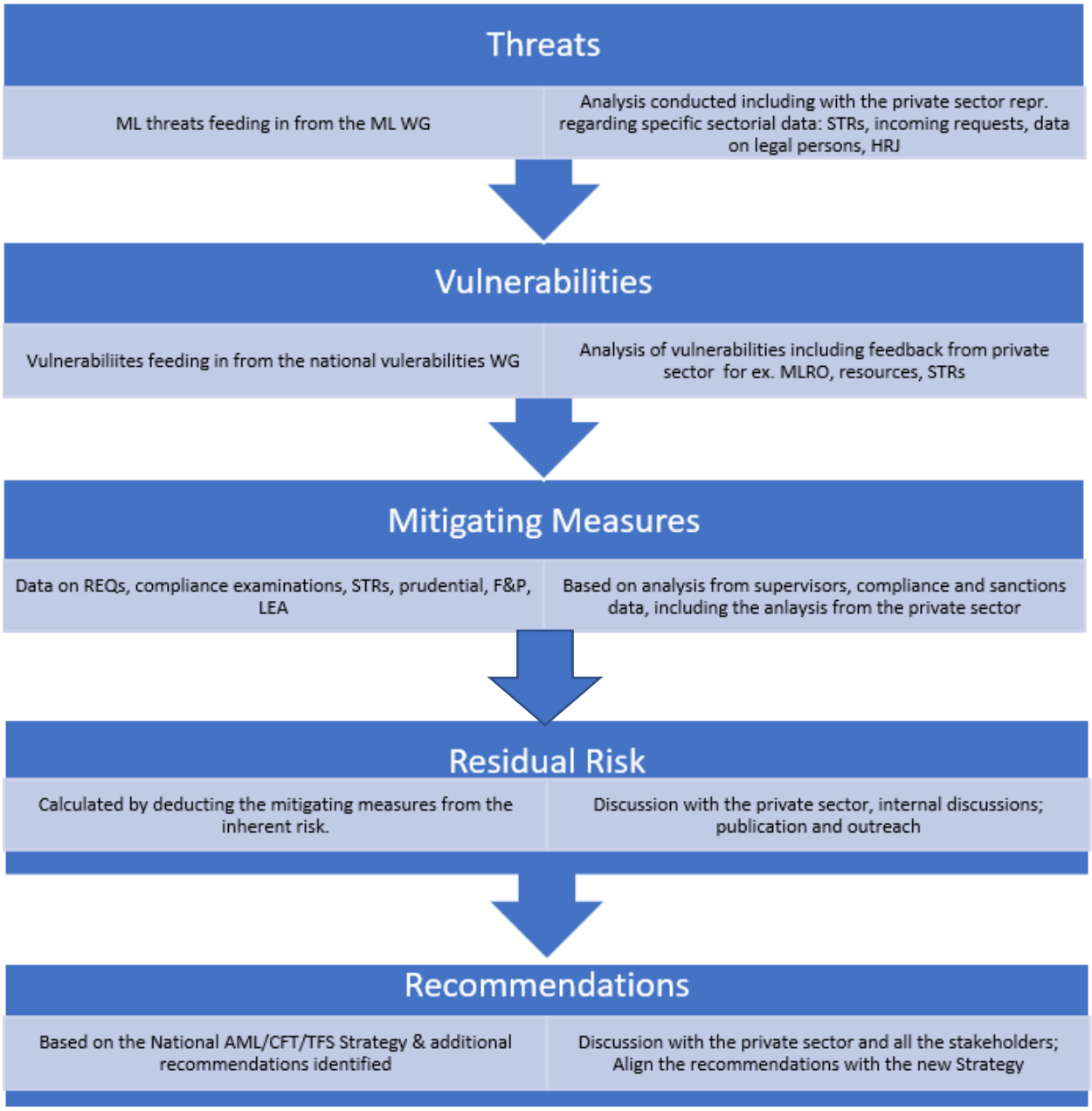
Different working groups were set up to assess the threats and vulnerabilities presented by a particular sector or area of activity. Each working group was composed of those authorities which have the most in-depth knowledge of the given sector, with one of them also assigned to lead the group. The said process has been improved considerably when compared to the one leading to the 2018 NRA and has led to a more detailed and accurate assessment of what are the main threats, vulnerabilities, and overall risks that Malta faces with respect to ML, TF, PF and TFS. From every working group, a detailed restricted working paper was produced, which fed into this publication. The following SWGs were created for the purposes of the NRA:

Table 5: List of sectoral working groups

	Chairperson	Participants
Financial sector working groups		
Banks	FIAU	MFSA, Malta Bankers Association, core banks, CBM, NCC
Financial Institutions (money remitters, payment service providers, e-money institutions)	MFSA	CBM, College of Stockbroking, Financial Institutions Malta Association, FIAU, NCC
Insurance	MFSA	FIAU, NCC, representative bodies
Pension schemes	MFSA	FIAU, NCC, College of Stockbroking, representative bodies
DNFBPs working groups		
Gaming	MGA	FIAU, NCC, private sector representatives.
TCSPs, Accountants, Auditors, Lawyers, and Tax Advisors	NCC	FIAU, MFSA, MBR, MTCA, Malta Institute of Accountancy, Chamber of Advocates, Accountancy Board, Malta Institute of Taxation, Institute of Financial Service Practitioners, private sector representatives
Dealing in High Value Goods	NCC	FIAU, MBR, Commerce Department, Transport Malta, MTCA, Malta Ship Registry, Customs Department, private sector representatives.
Immovables, notaries and real estate agents	NCC	Real Estate Licencing Board, FIAU, MTCA, Notarial Council, private sector representatives (including Malta Developers Association).
Virtual Financial Asset Service Providers (VFASPs), Virtual Financial Assets and new emerging technologies	MFSA	FIAU, ARB, OAG, MPF, NCC, private sector representative bodies

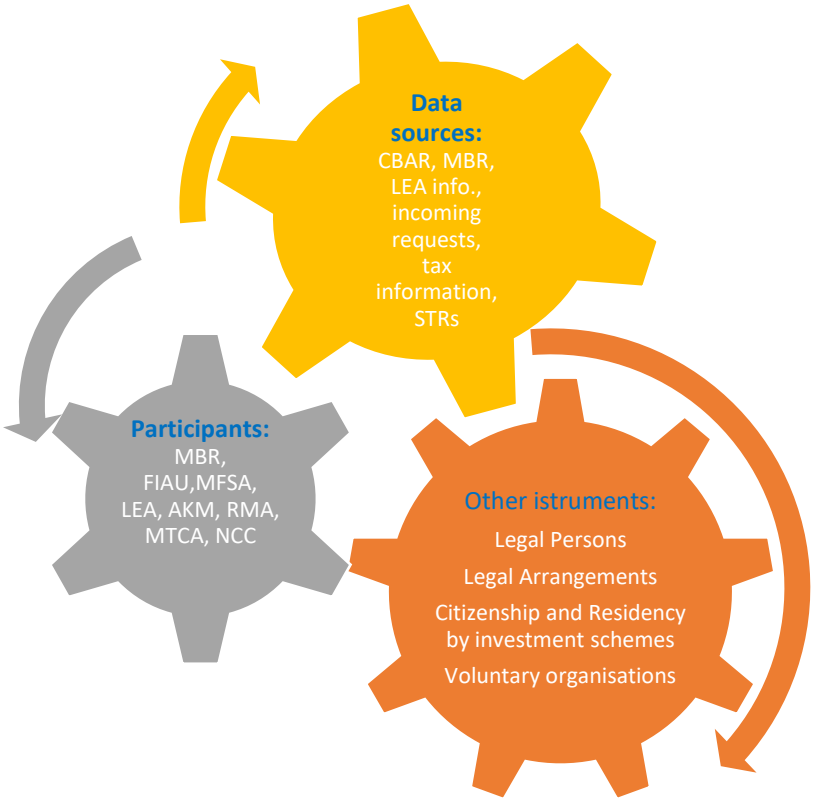
As indicated in Table 5, for financial institutions, DNFBPs and VFASPs, nine (9) SWGs were formed, which were formed in the following format as shown in Figure 8.

Figure 8: Outline of all the Sectoral Working Group Working Papers analysis, the results of which fed into the NRA



The following step was that of analysing the other instruments, which as shown in the following figure include the legal persons, the legal arrangements, the citizenship and residency by investment schemes, and the voluntary organisations. As shown in Figure 5, this analysis feeds into the ML threat working group and the vulnerabilities working group.

Figure 9: Analysis of the other instruments



The final process in the NRA involves the analysis of the contextual factors as shown in the following figure:

Figure 10: Contextual factors

Legislative & institutional	Size and materiality of the economy	Informal economy
• 2019 MER • 2021 Enhanced FUR •2021/2022 ICRG process • Capacity building • Strengthening good governance	• GDP & other economic indicators • Relative size of various sectors (FIs, DNFBPs, VFASPs) • Other instruments • Financial flows	• Size of the informal economy • Macroeconomic analysis • Cross-border cash flows

It is also to be noted that, in assessing TF, PF and TFS related risks, as well as other risk assessments that focus on ML with other predicate offences, high-risk countries and non-reputable jurisdictions that were taken into consideration were specifically considered for the purposes of

this NRA. For example, for the purposes of the TF risk assessment, the list of countries that fall under the category of high-risk jurisdictions was determined further to a thorough research aimed at identifying the jurisdictions considered to be either:
- state sponsors of terrorism
- the jurisdictions where terrorist groups are based or
- are known to be particularly active or in areas of conflict
- jurisdictions adjunct to the above.

7.1 Data sources

From the 2018 NRA onwards, all the supervisory and the law enforcement authorities as a result of a better ML/TF risk-based understanding, started adopting new techniques that assist further in the identification of the ML/TF threats. The primary starting point was to have a mapping of the data needed and to determine its availability. In fact, in the carrying out of the NRA, the different Working Groups leveraged additional data sources compared to what was the case with the 2018 NRA. Since the previous NRA, new databases have become available at the national level while competent authorities have significantly improved their data collection processes based on the past recommendations and lessons learned during the MONEYVAL and FATF process. Some of these additional and/or more accurate data sources include:

- Data obtained from the Beneficial Ownership Registers held by the MBR (for legal persons) and from Trusts Ultimate Beneficial Ownership Register (TUBOR) held by MFSA (for express trusts) such as the nationality and residence of individuals identified as beneficial owners.
- Data obtained from the Centralised Bank Account Register (CBAR)[16] held by the FIAU such as the nationality, residence or country of registration of accountholders and, where applicable, of their beneficial owners.
- Data sourced from the FIAU's Compliance and Supervision Platform for Assessing Risk (CASPAR)[17] system, and especially from its sector-specific Risk Evaluation Questionnaires (REQs).
- More granular data available to the FIAU's Intelligence Analysis Section through the goAML[18] system on suspicious transaction reports (STRs) submitted by subject persons to the FIAU, including on their quality and the predicate offence/s identified by subject persons, as well as data from the requests for information received by the FIAU, be they domestic or international in nature.
- Data from the supervisory and enforcement actions of the FIAU, MFSA, MGA, MBR, SMB, OCVO and MTCA.

[16] At the end of 2019 the FIAU was entrusted with the setting up and management of a centralised automated mechanism for the collection and retrieval of data on bank and payment accounts identifiable by IBAN, safe custody services (SCS) and safe deposit boxes (SDB) provided by credit and financial institutions within the Maltese territory. The CBAR system officially went live on the 26 October 2020 for data collection purposes. 31 subject persons (22 credit institutions and nine (9) financial institutions) qualified for CBAR reporting purposes and all such subject persons have registered and submitted data on their account holders, which data must be updated every seven days.
[17] In March 2019, the FIAU AML/CFT Supervisory Section adopted an efficient, standardised technology solution named CASPAR to facilitate the dynamic risk assessment of subject persons, risk data collection and risk scoring process. CASPAR system draws in data from a range of sources (such as submitted by reporting entities, supervisors, adverse media, NRA/SNRA, etc.) to allow for the comprehensive risk assessment of individual reporting entities.
[18] goAML was introduced in 2020 and this automated software system facilitates the submission of STRs and is developed by the United Nations Office on Drugs and Crime (UNODC).

- More accurate data from the OAG and the MPF with respect to Mutual Legal Assistance requests, European Investigation Orders, international cooperation, investigations of ML, TF, PF and TFS, with other predicate offences.
- International requests in relation to income tax and also international requests in relation to Value-Added Tax (VAT) from the MTCA.
- Data on the VAT registered traders involved in the acquisitions of goods and intra-Community supplies from the MTCA.
- More accurate data on assets seized, frozen and confiscated from the ARB.
- Data from the Commerce Department and Transport Malta that is further analysed if dealing with legal persons through the MBR registry.
- Data from the Central Bank of Malta on the international financial flows of banks and the money remitters.
- Data on the flow of funds via travelling from Customs Department (MTCA).
- Data on the activities carried out by the voluntary organisations that operate in conflict zones that have known links to terrorist groups or individuals from the OCVO.

The analysis of particular sectors has been substantially enriched through the data sources mentioned above, paving the way for a clearer understanding of the actual nature and level of ML/TF risks inherent thereto. By way of example, data from the beneficial ownership register and the CBAR is providing for a better understanding of the actual extent of foreign-owned legal persons that are not banking with local banks, possibly eluding having a financial footprint in Malta and making it harder for competent authorities to monitor and investigate their activities.

All data was sourced either directly from the respective authority or agency indicated above, or otherwise through data collected by the National Statistics Office. The cut-off date for the collection of data was 2021 and where available 2022. For the risk assessment on Company Service Providers (CSP), data reflects the new CSP regime in view of the legal amendments that came into force. Data in the legal persons' risk assessment is for 2022 in view of the risk assessment on the concealment of beneficial ownership carried out in 2021 and that fed into the analysis. The citizenship and the residency by investment schemes risk assessment present data for 2022 in order to ascertain any new trends in view of the actions taken as a result of the Russian Ukraine conflict. The PF and TFS risk assessment includes 2022 qualitative and quantitative information in view of the new sanctions regime imposed as a result of the Russian Ukraine conflict.

7.2 Threats

According to the FATF guidance on National ML and TF risk assessment[19], threat is a person or group of people, object or activity with the potential to cause harm to, for example, the state, society, or the economy. In the ML/TF context this includes criminals, terrorist groups and their facilitators, their funds, as well as past, present and future ML or TF activities. Therefore, threat is described as one of the factors related to risk.

[19] National money laundering and terrorist financing risk assessment (fatf-gafi.org)

The ML threats analysis in the 2023 NRA takes into consideration data regarding proceed generating predicate offences, typologies, and other information from the 2019 MER, the EU SNRA, and other bodies such as the EBA and the International Monetary Fund (IMF). As shown in the previous section, the assessment of the threats was conducted mainly in the ML threats working group complemented with findings from the sectoral working groups. The analysis included data and findings on:

- Proceed generating predicate offences
- ML, TF, PF and TFS related typologies (emerging from cases and internationally known typologies relevant to Malta as a financial centre)
- International requests – the police-to-police requests, the mutual legal assistance and European Investigative Orders, the FIU-to-FIU requests, international requests to/from the MTCA in order to understand the materiality of the threat, and the requests received and made by the MSS
- Freezing and confiscation of assets by predicate offence
- The suspicious transaction reports (STRs) and the Suspicious Activity Reports (SARs) received by the FIAU in two forms:
    - submitted by the subject persons/sector being assessed
    - concerning the subject persons/sector being assessed
- Inherent threats to Malta as a financial centre
- Findings from the EU SNRA
- Findings from the 2023 IMF Article IV consultation[20] that rates the high-risk sectors, such as gaming, virtual asset service providers, and activities that benefitted from Malta's Citizenship by Investment schemes with a likelihood and impact risk rating of 'medium'.

In addition, for the ML threat assessment and the TF risk assessment, an analysis of the international banking flows, the analysis of the financial flows from the money remitters and trade data was carried out in order to identify the outliers and analyse the implications of this analysis.

To determine the rating of the ML/TF threat, this update of the NRA also included the analysis on the consequence aspect. This is the approach that was explained by the Council of Europe (2013)[21], where the ML/TF threats are analysed as a combination of likelihood that the threat will occur and the impact of cost or damages if the threat occurs. In assessing the impact, the Council of Europe stresses that this is subjective and that in assessing the impact, countries are to take into consideration the financial loss to the business from the crime, the fines from the authorities, and the reputational damages to the country or sector. The overall matrix for assessing threats is as follows:

[20] Malta: 2022 Article IV Consultation-Press Release; and Staff Report (imf.org)

[21] Council of Europe (2013), Guidance Document for Risk-Based AML/CFT Supervision and for ML/TF Risk Assessment by Financial Institutions and DNFBPs.

Table 6: Matrix for assessing threats

Impact ► Likelihood ▼	Negligible	Minor	Moderate	Significant	Severe
Very Likely	Medium-low	Medium	Medium-high	High	High
Likely	Low	Medium-low	Medium	Medium-high	High
Possible	Low	Medium-low	Medium	Medium-high	Medium-high
Unlikely	Low	Medium-low	Medium-low	Medium	Medium-high
Very Unlikely	Low	Low	Medium-low	Medium	Medium

where on the likelihood:

- Very likely – implies that it occurs very often during a year
- Likely – probably occurs several times in a year
- Possible – probably occurs once per year
- Unlikely – unlikely to occur but not impossible
- Very unlikely – very unlikely to occur and highly improbable

With regards to the impact/consequence:

- Negligible – nil impact
- Minor – short-term or low consequence
- Moderate – medium term consequence
- Significant – long-term high consequence
- Severe – long-term significant consequence

Rating level of threat based on the above statistics and qualitative information is as follows:
1 – Low
2 – Medium-low
3 – Medium
4 – Medium-high
5 – High

7.3 Vulnerabilities

Vulnerabilities comprise those instances that can be exploited by the threat or that may support or facilitate its activities, where the focus is on factors that represent weaknesses in AML/CFT systems or controls or certain features of Malta. As shown in the previous section, the assessment of the vulnerabilities was conducted mainly in the vulnerabilities working group complemented with findings from the sectoral working groups. The analysis was based on the inherent vulnerabilities and the analysis of data from the FIAU REQs and the other qualitative and quantitative information held by the supervisory authorities, as well as taking on board relevant findings from the EU SNRA.

Vulnerabilities also include the features of the business/profession sector that make it vulnerable for ML, TF, PF and TFS purposes. The vulnerabilities are assessed with the following matrix, that takes into account the impact and the exposure to the specific vulnerability:

Table 7: Matrix for assessing vulnerabilities

Impact ► Exposure ▼	**Negligible**	**Minor**	**Moderate**	**Significant**	**Severe**
Very High	Medium-low	Medium	Medium-high	High	High
High	Low	Medium-low	Medium	Medium-high	High
Moderate	Low	Medium-low	Medium	Medium-high	Medium-high
Moderately Low	Low	Medium-low	Medium-low	Medium	Medium-high
Low	Low	Low	Medium-low	Medium	Medium

where on the exposure:

- Very high – implies that this takes place very often during a year
- High – probably occurs several times in a year
- Moderate – probably occurs once per year
- Moderately low – unlikely to have this vulnerability but not impossible
- Low – very unlikely to occur and highly improbable

With regards to the impact/consequence:

- Negligible – nil impact
- Minor – short-term or low consequence
- Moderate – medium term consequence
- Significant – long-term high consequence
- Severe – long-term significant consequence

Rating level of vulnerability based on the above statistics and qualitative information is as follows:
1 - Low
2 – Medium-low
3 – Medium
4 – Medium-high
5 – High

Here, the approach is in line with the EU SNRA where the *modus operandi* is taken into consideration in order to assess what is the exposure to the threats identified and the impact that such exposure can have. This assessment relied heavily on the data collected from the relevant supervisory authorities along with a qualitative analysis where necessary, in order to address any vulnerabilities from a legislative point of view.

7.4 Mitigating measures

In order to assess the effectiveness of mitigating measures in place, the approach adopted was two-fold:

a) An analysis of the controls put in place by regulators, through the supervision carried out both in terms of the checks at licencing and authorisation stage to prevent the entry of bad actors, as well as through ongoing monitoring, and when appropriate sanctioning, to ensure the subject person is operating in line with the salient legislative provisions. Guidance and outreach carried out were also taken into consideration, as well as the mitigating measures from the law enforcement authority.
b) An analysis of the AML/CFT compliance programs implemented by the subject persons themselves to prevent them from being used by their customers as a vehicle to facilitate the laundering of money or the funding of terrorism.

The rating of the effectiveness of mitigating measures is as follows:
1 – Low level – effectiveness achieved to a negligible extent. Fundamental improvements needed.
2 – Moderate – effectiveness achieved to some extent. Major improvements needed.
3 – Substantial – effectiveness is achieved. Improvements are needed.
4 – High – effectiveness is achieved to a large extent. Moderate improvements are needed.
5 – Very high – effectiveness is achieved to a very large extent. Minor improvements are needed.

Therefore, the highest rating of effectiveness is that of '5' and the lowest is that of '1'.

7.5 Inherent risk analysis

The inherent risk related to each threat and vulnerability was weighted by determining the likelihood and impact of any threat and the related likelihood and exposure of the vulnerability from materialising and the possible impact thereof. The resulting inherent risk rating resulted from the following risk matrix:

Table 8: Matrix for assessing inherent risk

Vulnerability ► Threat ▼	**Low**	**Medium-low**	**Medium**	**Medium-high**	**High**
High	Medium	Medium	Medium-high	High	High
Medium-High	Medium	Medium	Medium-high	Medium-high	High
Medium	Medium-low	Medium	Medium	Medium-high	Medium-high
Medium Low	Medium-low	Medium-low	Medium	Medium	Medium
Low	Low	Medium-low	Medium-low	Medium	Medium

7.6 Residual risk analysis

Further to the inherent risk analysis, the analysis focuses on assessing the effectiveness of mitigating measures implemented across the sectors. Given the analysis of the control measures, the residual risk for every sector is calculated through the following risk matrix. The overall

sectoral residual risk was calculated by taking a weighted average of the residual risk rating in the topics assessed.

Table 9: Matrix for assessing the residual risk

Inherent risk► Effectiveness of control ▼	Low risk	Medium-low	Medium	Medium-high	High risk
Low	Medium-low	Medium	Medium-high	High	High
Moderate	Low	Medium-low	Medium	Medium-high	High
Substantial	Low	Medium-low	Medium	Medium-high	Medium-high
High	Low	Medium-low	Medium-low	Medium	Medium-high
Very high	Low	Low	Medium-low	Medium	Medium

The residual risk rating is then as follows:

- 'Low' residual risk as a result of low inherent risk rating with highly effective mitigating measures that requires minimal improvements.
- 'Medium-low' residual risk is an inherent risk that is matched with substantial to very high mitigating measures, and minor improvements are required.
- 'Medium' residual risk is an inherent risk that is matched with mitigating measures that are not effective enough to mitigate against that risk, and thus more improvements are required.
- 'Medium-high' residual risk is an inherent risk that is matched with mitigating measures that are at mostly substantial, and where major actions are required.
- 'High' residual risk is an inherent risk that has correspondingly low or moderate effectiveness, and where actions require immediate priority.

8 Materiality and contextual factors

From the 2019 MER, Malta has shown political will and determination to address gaps identified in the AML/CFT framework and ensure its effectiveness. Apart from enhanced coordination, there were significant changes in the legal and regulatory framework. This section presents data on the materiality of various sectors, including, the relative importance of different parts of the financial sector, DNFBPs and VFASPs; the size and make-up of sectors; the amount of business which is domestic or cross-border; the extent to which the economy is cash-based; and estimates of the size of the informal sector. This section also presents other contextual factors that might significantly influence the effectiveness of a country's AML/CFT measures include the maturity and sophistication of the regulatory and supervisory regime in Malta; measures taken to improve good governance; and the level of financial exclusion. Such factors may affect the ML/FT risks and increase or reduce the effectiveness of AML/CFT measures.

8.1 Legislative and institutional framework

Since the onsite visit in Malta by MONEYVAL in 2018 adequate additional resources have been allocated and all the Maltese competent and law enforcement authorities have improved their

effectiveness in operations regarding AML and CFT, both on the preventative and ex ante controls. Cooperation and information sharing between the authorities, together with risk-based activities relying on improved risk understanding, have led to effective outcomes, which are now the focus of all the concerned authorities. This is evidenced in the following table that presents the level of resources in the financial supervision, the DNFBP supervision, the FIAU resources, the law enforcement, the other entities and the registries of legal persons and legal arrangements for the period between 2020 to 2022.

Table 10: AML/CFT human resources

	2020	**2021**	**2022**
Financial sector supervision – Number of full-time equivalent (FTEs) that carry out AML/CFT related duties			
FIAU	15	15	17
MFSA*	13	14	11
DNFBP supervision - Number of FTEs that carry out AML/CFT related duties			
FIAU	9	10	7
MFSA	Refer to above		
MGA**	76	75	78
FIAU			
Number of employees***	98	115	137
Law enforcement - FCID			
Number of employees dedicated to financial, including ML/TF, investigations	96	108	97
Office of the Attorney General			
Number of prosecutors	29	35	48
of which deal with financial crime		*20*	*22*
Legal procurators	2	2	2
Judiciary			
Magistrates	2	2	3
Judges	2	2	2
Other policy and coordination units (e.g., governmental organisations, ministries, etc.) – number of FTE that are tasked with AML/CFT affairs			
OCVO	-	5	10****
ARB	13	12	12*****
MTCA******	-	8	18
SMB	3	4	4
MBR (Legal persons)			
Number of FTEs that administer information related to legal persons (including support staff)	97	110	97
Number of FTEs that are tasked with AML/CFT affairs	48	49	55
MFSA (Legal arrangements)***** **			
Number of FTEs responsible for authorisation and prudential	19	19	19

** The MFSA has a Financial Crime Compliance (FCC) function/unit of which 13 (2020), 14 (2021) and 11 (2022) staff members are specifically assigned to direct AML/CFT supervision of both the financial sector and TCSPs (falling under DNFBPs). The rest of the function/unit, specifically the Offsite and Risk-Analysis team, is assigned to provide the necessary Financial Crime guidance, expertise and support to the other supervisory and also non-supervisory functions/units within the MFSA.*

***For the MGA:*

- *2020 data - of which 25 form part of the licence authorisation and criminal probity screening section, 38 form part of the compliance section (which represents the Investigations, Risk Management, AML, and other teams involved in regulatory supervision), 11 form part of the Legal and Enforcement and Policy, Outreach and International Affairs sections.*
- *2021 data - of which 19 form part of the licence authorisation and criminal probity screening section, 42 form part of the compliance section (which represents the Investigations, Risk Management, AML, and other teams involved in regulatory supervision), 12 form part of the Legal & Enforcement and Policy, Outreach and International Affairs sections.*
- *2022 data - of which 23 form part of the licence authorisation and criminal probity screening section, 42 form part of the compliance section (which represents the Investigations, Risk Management, AML, and other teams involved in regulatory supervision), 13 form part of the Legal & Enforcement and Policy, Outreach and International Affairs sections.*

****For the FIAU:*

- *2020 – Intelligence Analysis Section – 30; Supervision – 26; Enforcement – 9; Other Sections – 33*
- *2021 – Intelligence Analysis Section – 32; Supervision – 32; Enforcement – 9; Other Sections – 38*
- *2022 – Intelligence Analysis Section – 35; Supervision – 36; Enforcement – 15; Other Sections – 51*
- *To note that the discrepancy between the breakdown in the numbers of supervision of FIs and DNFBPs and the total figure of supervision is due to the fact that the broken down numbers only include FTEs during supervision of the financial sector and DNFBPs, and do not include administrative staff and the risk team which form part of the total number of staff in supervision.*

*****Includes pre-enrolment/annual returns / legal and compliance services.*

******Does not include another 2 ARB employees seconded to other ministries (unrelated duties)*

*******MTCA:*

- *During 2020, all accountants and seniors used to work on both, administrative and criminal tax cases. The change came in 2021/2022.*
- *In 2021 there were 4 inspectors and 4 accountants*
- *In 2022 there were 3 Senior Accountant/Managers, 10 Accountants, and 5 Revenue Inspectors*
- *The above assist FCID and FIAU in tax crime cases*

********The MFSA has a dedicated function/unit responsible for the authorisation and prudential supervision of Trustees and Company Service Providers. The figures provided are the total FTEs of this function/unit who are therefore responsible for both sectors (including the responsibility for the register of beneficial owners of trusts [TUBOR]).*

In addition, it is to be noted that the FIAU increased the expenditure on technological equipment from €14,773 in 2017 to €1.8 million in 2020, and €1.6 million in 2022.

With regards to the legislative AML/CFT framework, in April 2021[22], Malta achieved a re-rating by MONEYVAL in the nine recommendations on which it had been originally rated partially compliant in the 2019 Mutual Evaluation Report[23]. Malta succeeded in achieving a re-rating in the recommendations to compliant or largely compliant in relation to:

- non-profit organisations,

[22] 1680a29c70 (coe.int)
[23] 168097396c (coe.int)

- correspondent banking,
- new technologies in the form of virtual financial assets,
- the reporting of suspicious transactions,
- transparency and beneficial ownership of the legal persons,
- regulation and supervision of financial institutions and
- regulation and supervision of DNFBPs,
- international instruments, and
- mutual legal assistance in terms of freezing and confiscation.

These are all key areas for a robust AML/CFT framework. In addition to this re-rating, Malta continued to assess its robustness in the legal framework. In fact, in 2021, Malta introduced the use of cash restrictions legislation, as well as the Proceeds of Crime Act (Act V of 2021)[24] which was published on the 19 February 2021 and came into force on the 12 March 2021. The Act provides for the identification, tracing, freezing and confiscation of proceeds of crime including laundered property, income and other benefits derived from such proceeds held by criminal defendants, property that is the proceeds of, or used in, or intended or allocated for use in the financing of terrorism, terrorist acts or terrorist organisations, for the setting up of the Asset Recovery Bureau as a body, independent from the Government and for setting out the procedure for non-conviction based confiscation of proceeds of crime. In addition, Subsidiary Legislation 233.07[25] was amended, as of 7 July 2020 thus enabling the Commissioner for Tax and Customs to detain any cash, whatever its value, whether it is being carried or unaccompanied, and whether it has been declared or not, where there are indications that the cash is related to criminal activity. This allows the Customs Department (MTCA) to restrain cash for a determined period pending investigations.

Apart from legal and institutional reform measures, several other measures of capacity building and of strengthening anti-corruption structures have also been implemented or are in the process of being so implemented. These reforms involve the increase of the resources of the Police to investigate economic crime, the increase in resources of the FIAU, the MFSA and the MGA as evidenced in Table 10, as well as the separation of the investigative and prosecutorial roles of the Police. The latter involved the transfer of prosecution powers before the Courts of Magistrates which were previously exercised by the Police, to the Office of the Attorney General. This is being done through a phased and a gradual, albeit accelerated, process. Amongst the first categories of crimes the prosecution of which passed with effect from the 1st of October 2020 was to pass to the Office of the Attorney General crimes of ML, economic crimes, evasion of customs and excise duty, terrorism and TF, and corruption. This process also involved a capacity building process in the Office of the Attorney General through an extensive recruitment process.

Malta's mitigating measures to enhance good governance include substantive laws which render various forms of corruption a criminal offence, laws which exclude the time barring of corruption offences in certain circumstances, civil laws which provide for an action for damages suffered as a result of corruption and procedural tools which encourage witnesses to come forward in reporting and in giving evidence on corruption offences, as well as other measures regarding Politically

[24] LEĠIŻLAZZJONI MALTA (legislation.mt)
[25] LEĠIŻLAZZJONI MALTA (legislation.mt)

Exposed Persons (PEPs)[26] as part of the AML/CFT preventative measures, and other steps taken to preserve and improve the high level of integrity of all branches of government in Malta. These steps have all been enhanced in recent years. There are several legal amendments that mitigate against corruption. Amendments to the Constitution and to other laws on the offices of the Ombudsman, the Auditor General, the Commissioner for Standards in Public Life and the Permanent Commission Against Corruption have given those institutions the power to report findings of acts of corruption directly to the Attorney General for prosecution. Any decision by the Attorney General not to prosecute such cases may be judicially reviewed at the request of those institutions which, for the purposes of the law on judicial review of such decisions, are given the same status as victims. The Public Administration Act, 2019, establishes Codes of Ethics for employees in the public sector and makes a breach of those Codes a disciplinary offence without prejudice to criminal liability. In December 2019 a Code of Ethics for public prosecutors at the Office of the Attorney General was published. Moreover, in 2021 the contracts of employment of new recruits at the Office of the Attorney General were revised in order to include a revolving door clause. Malta is committed to continue monitoring and further strengthening of the rule of law, as even recommended through the membership with the Group of States against Corruption (GRECO).

8.2 Size and materiality of the economy

The Republic of Malta is a Southern European Island country, member of the EU, comprising an archipelago in the Mediterranean Sea. It lies 80 km south of Italy, 284 km east of Tunisia, and 333 km north of Libya. The country covers just over 316 km^2 with an estimated total population at the end of 2022 of 542,051, up by 5% when compared to 2020, making it one of the world's smallest and most densely populated countries.

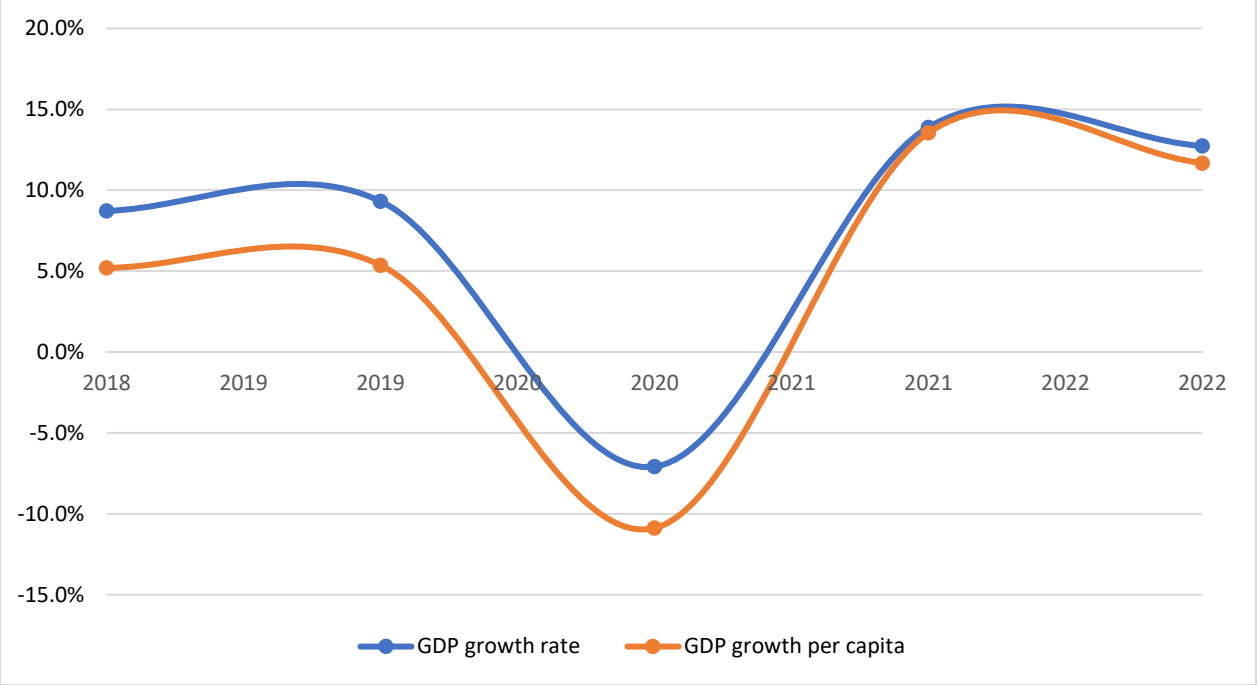
As assessed by the 2022 Article IV Consultation-Staff Report[27], Malta's economy rebounded strongly from the pandemic[28]. Total Gross Domestic Product (GDP) in Malta in 2022 stood at €16.9 billion, with a growth rate of 11.7% from the 2021 level. GDP growth per capita increased by 12.7% from 2021 to 2022 as shown in the following figure.

[26] Government Notices published in Govt. Gazette No. 20,602 of 6th April 2021

[27] Malta: 2022 Article IV Consultation-Press Release; and Staff Report (imf.org)

[28] IMF reports as well that although, the indirect impact of Russia's war in Ukraine, including the anticipated slowdown in the European economy, high and volatile global energy prices, rising import costs, and weakened public finances following the pandemic are weighing on the outlook.

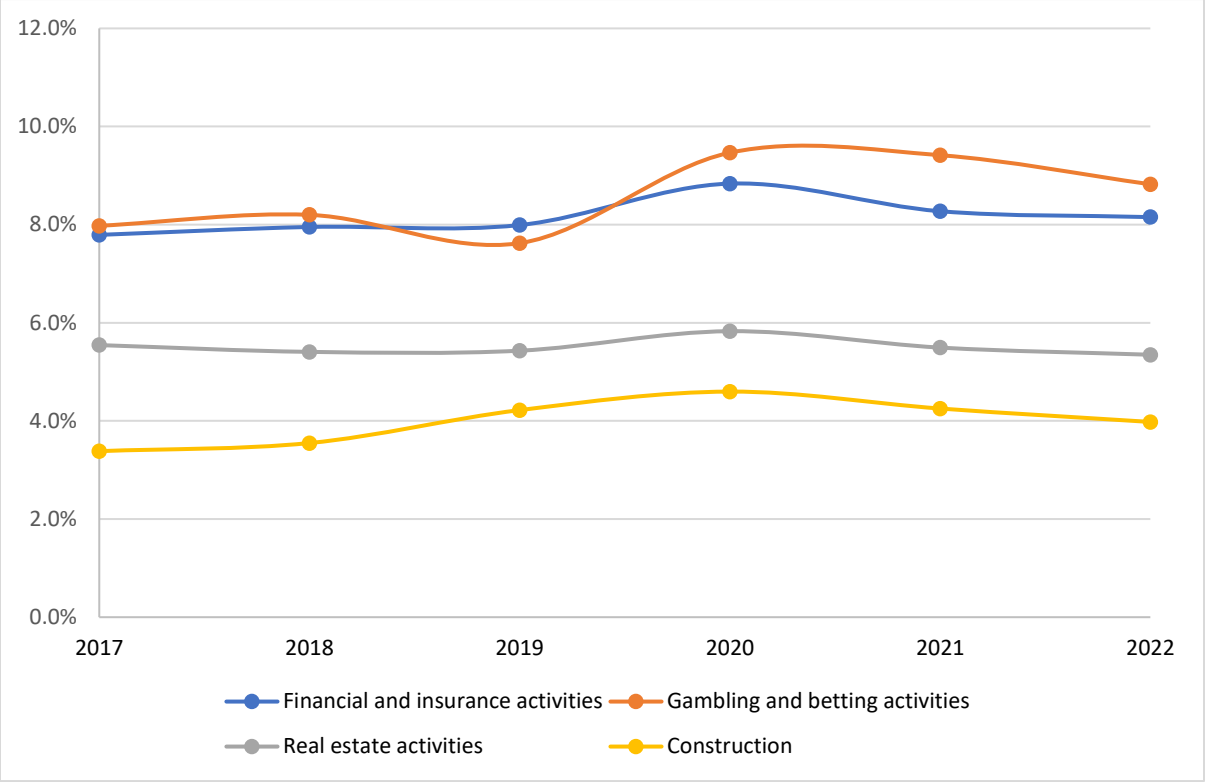
Figure 11: GDP growth in Malta



Source:
Data of 2017 is in line GDP News Release NR218/2022 published on 29 November 2022.
Data of 2018 onwards is in line GDP News Release NR095/2023 published on 30 May 2023.
Population – NSO data

Figure 12 presents the percentage share of GDP of specific sectors in the Maltese economy, (financial and insurance, gambling and betting, real estate, and construction). In 2022, the gambling and betting activities sector accounted for the highest percentage share of GDP.

Figure 12: Key sectors with their percentage share of GDP



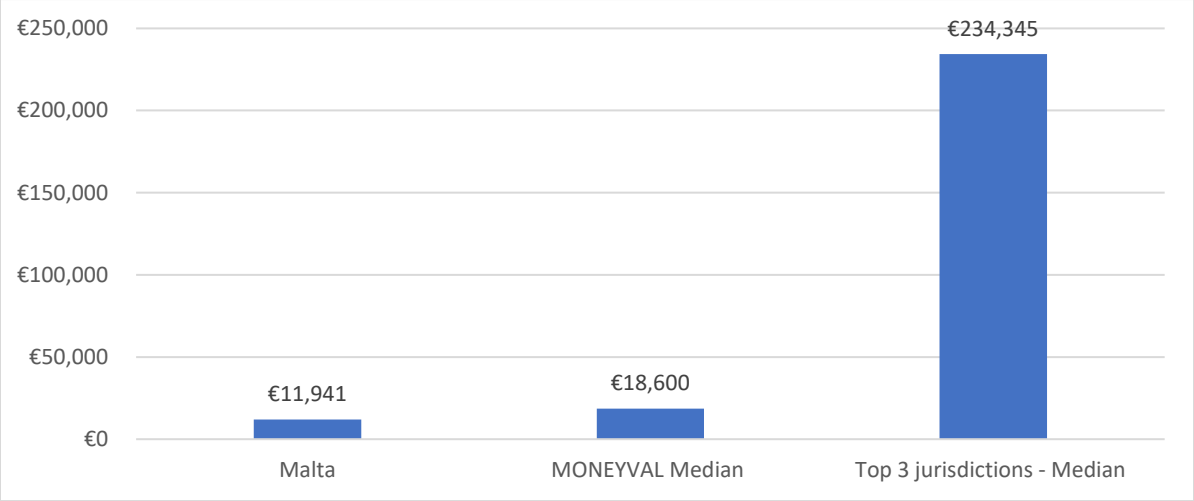
Source:
Data of 2017 is in line GDP News Release NR218/2022 published on 29 November 2022.
Data of 2018 onwards is in line GDP News Release NR095/2023 published on 30 May 2023.

In terms of employment, in 2022, NSO data indicates that the financial and insurance activities sector accounted for 4.6% of the full-time equivalent gainfully occupied, while the gambling and betting activities accounted for 2.9%.

The statistics on materiality that MONEYVAL presented in the respective working group and that will eventually be used in the 6th round of evaluation procedures, also indicate that Malta is not comparatively a large financial centre. Data on all the jurisdictions indicate that in terms of GDP in million Euro for 2020, the figure for Malta (Eur11,941 million) is below the median of the jurisdictions[29], as well as below the top three jurisdictions[30], as shown in the following figure.

[29] Jurisdictions included are Azerbaijan, Albania, Lithuania, Montenegro, Ukraine, Serbia, North Macedonia, Poland, Slovenia, Czech Republic, Hungary, Latvia, Monaco, San Marino, Estonia, Georgia, Bulgaria, Armenia, Croatia, Cyprus, Malta, Andorra, Liechtenstein, Romania, Moldova, Gibraltar, Isle of Man, Jersey, Guernsey, Bosnia and Herzegovina, Holy See, Slovak Republic.
[30] These are Poland, Romania, and Czech Republic.

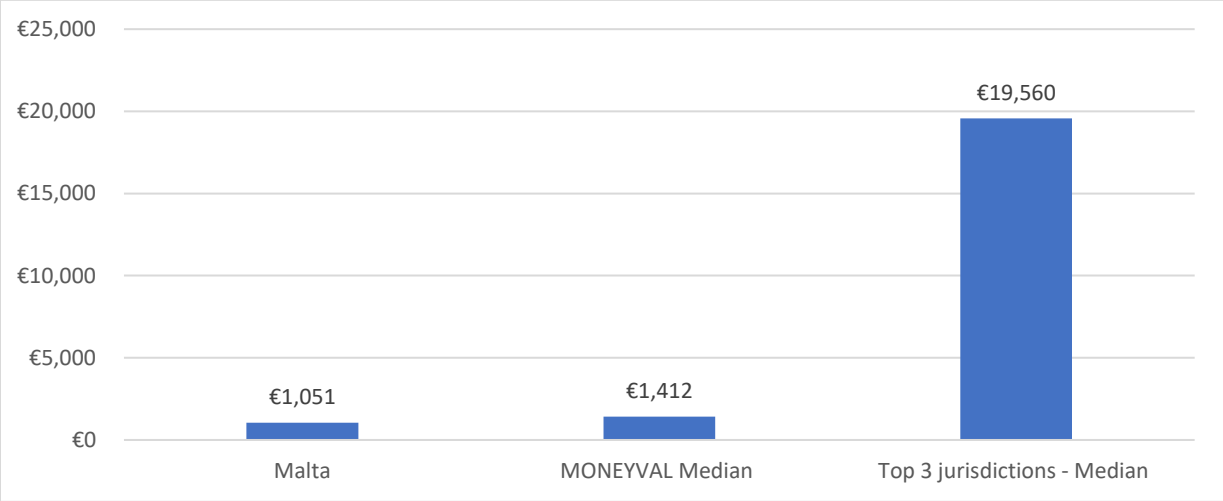
Figure 13: GDP in million Euro (2020 figures) - materiality



Source: MONEYVAL

In terms of the size of the financial sector in million Euro, as shown in the following figure, Malta's size is lower than the MONEYVAL jurisdictions' median[31], and much below the figures presented for the top three jurisdictions[32] in this category.

Figure 14: Size of the financial sector in million Euro (2020 figures) - materiality



Source: MONEYVAL

8.3 Size and materiality of the various sectors

The 2019 MER[33] in the assessment of the materiality and level of ML/TF risks of the different FIs and DNFBPs presented the following categories:

[31] Jurisdictions included are the same under footnote 35.
[32] These include Romania, Poland, and Czech Republic.
[33] Moneyval-Mutual-Evaluation-Report-Malta-2019 (25).pdf, par. 65.

a) *most significant*: the banking sector based on the overall market share, as well as known ML/TF typologies; TCSPs given their international client base, involvement with complex corporate structures and legal arrangements and the fact that not all TCSPs are registered.

b) *significant*: remote gaming companies based on the high number of customers, mainly non-resident, the high volume of transactions, the non-face-to-face nature of the business and the use of prepaid cards; real estate agents due to their involvement in Malta's Individual Investor Program (IIP)[34] and lack of registration requirements; accountants and legal professionals (both lawyers and notaries) based on exposure to ML/TF risks; and virtual assets.

c) *less significant*: other FIs, including securities providers and insurance, and other DNFBPs.

Taking into account all the analysis that was carried out in this iteration of the NRA, the assessment of the materiality presented in the 2019 MER calls for some revisions in the components of the categories. For instance, in view of the deficiencies that were addressed in the TCSPs sector, the effectiveness of the licensing and authorisation is considered as 'very high' (the highest rating for the effectiveness of mitigating measures) and therefore, the deficiency identified in the 2019 MER is to be considered as addressed. In fact, this is as a result of the fact that whilst until 2020 a number of professionals (such as warranted lawyers and accountants) and individual service providers providing directorship and company secretary services below certain thresholds were exempt from MFSA licensing, through legislative amendments published in 2020[35], these have now also been captured within the MFSA's licensing and supervisory remit, and therefore required to undergo the same fitness and propriety assessments as well as ongoing scrutiny by the MFSA. In recent years, therefore, there has been a drive by Maltese authorities to raise the bar for all persons providing such services by harmonising the market entry requirements and reducing and eliminating existing gaps, increased AML oversight by both FIAU and prudential regulators, as well as increasing enforcement action through sanctioning or remediation plans, depending on the severity of the breaches identified.

Furthermore, insofar as estate agents, property brokers, branch managers and property consultants are concerned, the Real Estate Agents, Property Brokers and Property Consultants Act, 2020[36] was enacted with the objects and reasons being to streamline persons acting as intermediaries in the process of negotiating and arranging transactions involving the acquiring or disposing or leasing of land and in doing so, provide for better protection of consumers and prevention of crime and fraud that may be associated with such activities. This essentially, enabled the licensing of real estate agents, branch managers and property consultants working for real estate agents as well as property brokers and addresses the conclusion made by MONEYVAL with regards to the lack of registration requirements.

On the other hand, with regards to FIs being less significant, in the analysis carried out, the FIs sector as a result of the de-risking has seen an increase in the number of clients onboarded and therefore this sector should now be categorized under a different category rather than under the category of 'less significant'.

[34] Now referred to as citizenship by investment scheme.
[35] LEĠIŻLAZZJONI MALTA (legislation.mt)
[36] LEĠIŻLAZZJONI MALTA (legislation.mt)

Furthermore, this section presents salient quantitative information on the materiality of the sectors categorised above. Primarily, the financial sector in Malta has developed deep expertise in certain areas along the years. According to the Bank for International Settlement (2022)[37], *a financial centre is a location, usually a city or district, where intermediaries involved in the provision of financial services are concentrated. In so far as it is open to foreign participants, any financial centre can be considered international*. This study classifies Malta as a global financial centre in the group of countries that in 2020, feature the highest US dollar value of cross-border financial intermediation with the ratio to GDP higher than the cross-country median, but lower than the median of the cross-border centre. In addition, ranking by cross-border financial intermediation ratio (minimum of external assets and liabilities as a ratio to GDP) showed Malta as one of the countries that moved into the cross-border financial centre group over the 1995-2020 period. This study sustains Malta's contextual factor of being an island with a financial sector that accounts for a significant share of the economy. This contrasts with the findings presented above from the statistics on materiality project by MONEYVAL.

By providing an extensive range of products and services to retail, corporate, institutional, and private banking customers, Maltese banks play a crucial role in supporting the economic activity in Malta. Banks are also a key channel for international transactions into and out of Malta. In aggregate, as at end of 2022, the Maltese credit institutions were servicing some 1.4 million customers (2021: 1.3 million). The core domestic banks have a traditional business model and are largely funded by resident deposits with most of their assets representing claims on residents. The six (6) non-core domestic banks, which undertake some business with Maltese residents, but not as their core activity, hold €3 billion of assets (20% of GDP). The ten (10) international banks hold €11 billion of assets (73% of GDP) and are mainly subsidiaries and branches of international institutions, with almost no links to the domestic economy.

The FIs sector has experienced a sizeable growth both in terms of number of licence holders and business volume, mainly in so far as payment services institutions (PIs) and electronic money institutions (EMIs) are concerned, where a total of ten (10) financial institutions were licenced during the three-year period ending 2022. The sector is growing significantly both in terms of number of licence holders and business volume. The growth, which is mainly in PIs and EMIs, is a result of Malta's placement as a jurisdiction which favours financial innovation as well as by a number of UK PIs and EMIs migrating their business to Malta following the UK exit from the EU. This was countered by a higher incidence of surrendered licences (12). The increased voluntary surrenders are a direct consequence to the sustained supervisory presence in 2020 and 2021 leading to significant supervisory and regulatory action.

Another significant sector in Malta is the gaming sector, which has rapidly grown over the past twenty years. Gaming consists of four (4) land-based companies and 453 licensed remote gaming companies. At the end of 2022, the number of companies licensed by the MGA and operating in Malta, including online and land-based entities, stood at 350. Gaming licences issued by the MGA amount to 358, as well as 329 approvals to offer various types of games under the Business to Customer (B2C) licence, and 206 approvals to offer services under the Business to Business (B2B) licence.

[37] https://www.bis.org/publ/qtrpdf/r_qt2206b.pdf

Company service providers (CSPs) have a significant role in Malta especially in view of the fact that for example, in 2022, 91.5% of the legal persons in Malta were incorporated by a company service provider (CSP). It is to be noted that the CSP as a sector recorded a decrease in the population from 2021 to 2022. This decline reflects the more onerous obligations, particularly on prudential and governance obligations as well as minimum capital requirements. The amendments to the CSP licensing regime[38] provided for the following:

- Inclusion of lawyers, notaries public, auditors and accountants, within scope of the CSP Act and subject to adequate market entry requirements and proportionate on going fitness and propriety and compliance requirements
- Including service providers that were previously exempt under the "de minimis" rule within the scope of the CSP Act and the market entry requirement and making them subject persons; and
- Strengthening the ongoing requirements applicable to CSPs with regard to Governance, Risk Management, Compliance and Time Commitment addressing relevant outcomes of the sectoral risk assessment.

Furthermore, with the amendments, another introduction was that of categorising the TCSPs into classes by reference to the business model and scope of services provided to reflect the differences in the risks posed by that business model.

The VFAs landscape in Malta has changed considerably along the years. In assessing the landscape of the VFA service providers it is interesting to note the whole process from 2018 up to 2021, where in November 2018, 180 entities notified interest to the MFSA. By October 2019, there were 89 declarations of cessation of business, and 34 VFASPs submitted a Letter of Intent, 6 (six) of which did not actually materialise into a submitted application. Subsequently, there were 57 warnings issued and entities struck off by the Malta Business Registry. All issues encountered by the supervisory authorities in Malta were proactively shared with other jurisdictions whereby such operators had a footprint. As at end 2022, there were 11 authorised VFASPs in Malta. During 2021, the VFASPs sector attracted six (6) million clients, which are mostly retail, with approximately 56% of such clients being considered as active[39]. Out of these clients, 99.8% are non-resident clients. These licensed VFASPs held €17.9 billion of assets under custody and had a total trading volume of €357 billion.

Investment services in 2021 had 55.7% non-resident clients. Money Value Transfer services that had 56.1% of the total value of transactions with foreign countries, while banks had 14.8% of the total value from non-resident clients.

These figures, indicate that in terms of clients, apart from the VFASPs, banks and investment services have their number of clients almost divided equally between non-resident and resident clients. With regards to the clients' deposits, the banks' deposits are the majority from the resident clients.

Therefore, in view of the key findings presented above from the materiality analysis that was carried out for every sector, the materiality of the various sectors, taking into account the turnover,

[38] https://parlament.mt/en/13th-leg/acts/act-l-of-2020/

[39] That is, clients who have carried out at least one transaction in the previous six-month period.

the number of transactions, the number of foreign clients, the assets under management, the contribution to the overall GDP, is as follows:

a) *Most significant*: the CSPs given the number of legal persons in Malta and their exposure to international client base, the banking sector based on the overall market share, as well as known ML/TF typologies, the remote gaming companies based on the high total value of transactions, number of customers, mainly non-resident, and VFAs in view of the international client base and the total value of transactions. FIs are also categorised here in view of the increase in the volume and value of their international activity.

b) *Significant*: the legal arrangements and their exposure to international client base; and sectors dealing with immovable property[40], and the high-value goods.

c) *Less significant*: pensions, securities providers, and insurance, and other DNFBPs[41] including accountants and legal professionals (when these do not perform corporate related services), and as well, the land-based gaming.

8.4 Financial flows analysis

For the purpose of the 2023 NRA, a financial flows analysis was carried out in the relevant working papers, in order to fully assess the ML and TF threats.

In the ML analysis, two indicators were used to identify the outliers in the net banking flows sent to Malta: those with an amount exceeding the Eur10 million per year, and those jurisdictions that when compared to the asset loans, incoming remittance payments, and exports of goods and services, and there was no trade activity (goods and services). For these jurisdictions a further analysis was done, that focused on identifying any involvement of legal persons registered in Malta, with the analysis identified the residence of the BOs and the residence of the shareholders of the legal persons registered in Malta, and the foreign direct investment in the form of paid-up share capital had. The residency of the beneficial owner and the shareholders was taken into consideration in order to align with the banking regulations definition of 'residency'[42].

Net banking flows sent to foreign jurisdictions from Malta were also assessed and compared with the remittances data and the trade data in order to identify the outliers. In this analysis, the outliers were those that show movement of funds from the credit institutions in Malta or remittance payments to jurisdictions that are considered as high-risk countries for TF purposes and with which there is no trade activity. An important conclusion made here was that the TF higher risk countries with which there are flows and no trade activity are featuring under the financial remitters rather than the credit institutions. In the analysis on the outgoing remittances, the number of persons residing in Malta who are nationals of high-risk countries was also taken into consideration, using as a source of data, Identity Malta.

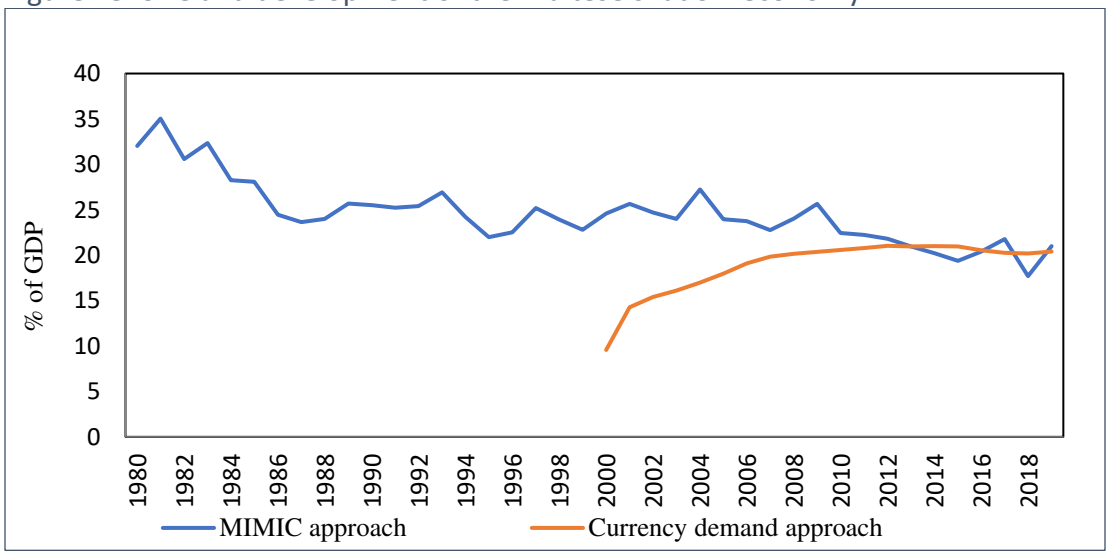
[40] Real estate agents should be considered less significant in the Maltese context due to their limited role. The detailed analysis in 'section 10.2.6'.
[41] When these do not perform corporate related services.
[42] A full definition of what is meant by 'residence' in this context is found in Appendix 2 of the BR06 guidelines https://www.centralbankmalta.org/site/excel/statistics/BR06-instructions.pdf?revcount=5376.

The relevant findings from the analysis regarding financial flows analysis including specific ML/TF high-risk jurisdictions will be conveyed to the relevant entities via public private partnerships. As indicated in the FIAU Implementing Procedures in section 8.1.2[43], information regarding high-risk jurisdictions should go beyond the non-reputable jurisdictions and include other reliable sources.

8.5 Informal economy

In a study that was published by the Central Bank of Malta[44], by using both the macro method, Currency Demand Approach (CDA) and Multiple Indicators Multiple Causes (MIMIC), it was found that Malta's shadow economy was estimated to range between 15.3% and 23.6% of GDP, depending on the calculation method used. While the two methods give a somewhat different indication about the trend in the size of the underground economy before 2010, reflecting differences in the underlying assumptions and methodology, the results for more recent years are very similar. Indeed, both estimates show that the size of the underground economy in Malta has been quite stable, with the MIMIC measure also showing a slight downward trend as shown in figure 15. Figure 15 shows that both estimates show that between 2008 to 2018, the size of the underground economy in Malta has been quite stable, with the MIMIC measure also showing a slight downward trend.

Figure 15: Size and development of the Maltese shadow economy



Source: Central Bank of Malta

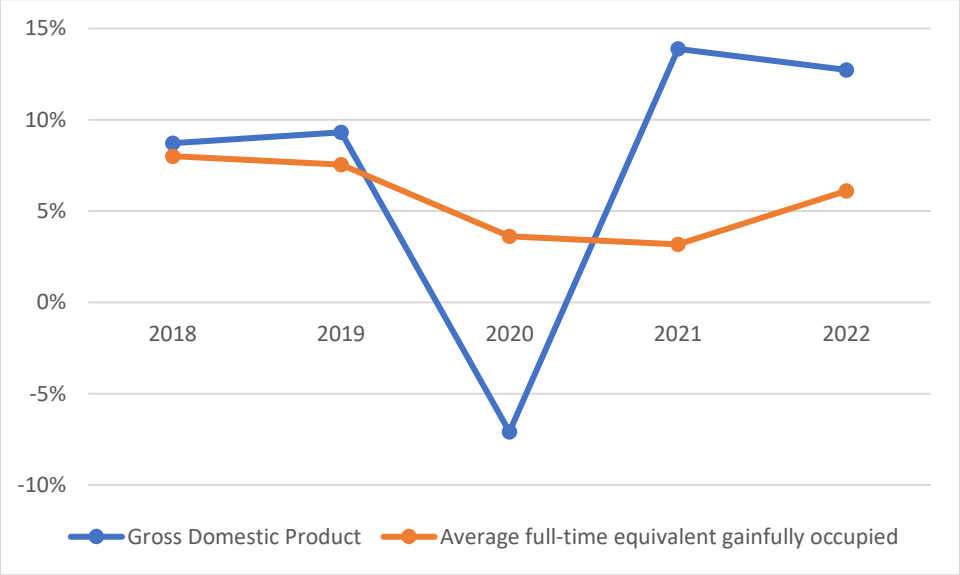
This decrease in the informal economy was also captured through a COVID-19 related measure, the wage supplement measure. The 2018 NRA for Malta considered that one of the main sectors that appeared to attract undeclared work was tourism (including hotels and restaurants). Under the wage supplement measure, businesses and the self-employed that are directly dependent on the

[43] Layout 1 (fiaumalta.org)

[44] Central Bank of Malta (2020), An analysis of the shadow economy in Malta: A Currency Demand and MIMIC model approach - WP/02/2020.

tourism industry (tourist accommodation, travel agents, language schools, event organisers and air transport operators) received a wage supplement. For this measure to apply, the relevant work had to be declared and consequently the wage supplement measure was an incentive for the companies and their workers to join the formal economy. This effect is in fact evidenced when one compares the percentage growth in GDP and the percentage growth in employment as shown in the below figure for up to 2020. However, in 2021 we see a significant rise in the GDP growth which is corresponded by a decline in the employment growth albeit still a positive employment growth rate. This may indicate that the there is a shift towards the informal economy again as pre wage supplement measures. As shown in Figure 16, from 2019 to 2020, growth in employment has increased at a decreasing rate whereas growth in GDP has decreased over the same period from 2019 to 2020. Therefore, the increase in employment is not explained by an expansion in the economy, which therefore implies that there was a shift from the informal economy to the formal economy. However, in 2021 this correlation is not evident as indicated in figure 16. The informal economy enables tax crime and as argued by IMF (2002)[45], the size of the shadow economy is a core input for the estimation of the extent of tax crime and thus for decisions on its adequate control.

Figure 16: Percentage growth in GDP and percentage growth in employment



Source: National Statistics Office

This analysis led to the conclusion that Malta has an informal economy (with a decreasing trend) which is significant to AML/CFT risks.

8.6 Cross-border cash declaration

Data from the MTCA also shows that there are a significant number of declared cash at the border, as shown in the following tables:

[45] https://www.imf.org/external/pubs/ft/issues/issues30/

Table 11: Declared cash incoming and outgoing

	Entering Malta		Leaving Malta	
	Declarations	**Sum €**	**Declarations**	**Sum €**
2013	5,344	251,941,837	889	52,556,813
2014	2,816	99,895,902	815	44,970,209
2015	713	28,035,843	307	20,360,093
2016	261	12,340,651	182	5,933,148
2017	166	15,864,432	331	18,625,346
2018	131	5,229,768	420	11,829,636
2019	107	3,921,939	542	23,536,945
2020	45	1,776,918	304	15,180,573
2021	51	1,439,649	321	9,796,895
2022	85	1,718,619	382	9,229,183
Totals	**9,718**	**422,259,641**	**4,494**	**211,957,867**

Source: MTCA

Table 12: Cases of undeclared cash

Year	**Undeclared cash**	
	Number	**Amounts €**
2013	4	595,145
2014	1	23,000
2015	1	41,400
2016	2	72,971
2017	10	214,440
2018	10	203,335
2019	66	1,547,116
2020	40	655,722
2021	46	851,306
2022	56	843,394
Totals	**232**	**5,047,829**

Source: MTCA

Through the Cash Control Regulations, Subsidiary Legislation 233.07[46] any person entering or leaving Malta or transiting through Malta and carrying a sum equivalent to €10,000 or more in cash (or its equivalent in other currencies) is obliged to declare such sum to the Commissioner for Tax and Customs, in an applicable Cash Declaration Form. As can be assessed from table 11, from 2017 onwards outgoing cash is higher than incoming cash thus implying that the threat of laundering foreign proceeds of crime in Malta via incoming cash declarations/undeclarations is low since outgoing cash is higher than that incoming. However, it is to be noted that actions by the authorities, including, the checks carried out by the MTCA, FIAU strategic analysis, investigations by the Malta Police Force, and the prosecutions by the Office of the AG, all led to less cash being moved as is evidenced by the decline in the figures of the outgoing cash that declined to

[46] https://customs.gov.mt/docs/default-source/travellers/233-07.pdf?sfvrsn=2

€9.2million by 2022. Nonetheless, the threat of such laundering of money via the use of cash still exists.

9 Other instruments

This section presents the results of the following risk assessments that are key in the context of the Maltese economy and are referred to as 'other instruments' in this NRA:

- Legal persons
- Legal arrangements
- Citizenship and residency scheme by investment
- Voluntary Organisations

Subject persons are to assess their risks not only based on the analysis in their respective sectoral section, but also on additional sections, such as, the overall ML risks 'section 11', 'section 12' that presents the TF risks, 'section 13' on PF and TFS related risks, as well as the other instruments as described in this section.

9.1 Legal persons

This section presents the results of the legal persons'[47] risk assessment, that includes also the risks in relation to the foundations and associations. This risk assessment builds on the interim risk assessment that focused on assessing the ML/TF threats of commercial partnerships with a specific focus on beneficial ownership, that was carried out in August 2021 and that was submitted to the FATF as part of the actions taken to address the FATF action plan for Malta. This risk assessment was key to enhance MBR's risk understanding on the potential misuse of legal persons and concealment of beneficial ownership. In August 2021, the 'high-risk' legal persons for concealment of BO for ML purposes, were those that do not have the involvement of Maltese resident directors, have complex and multi-layered structures and lack a Maltese IBAN account.

As indicated in the introduction to this section, subject persons are to assess their risks not only based on the analysis in their respective sectoral section, but also on additional sections, such as, the overall ML risks 'section 11', 'section 12' that presents the TF risks, 'section 13' on PF and TFS related risks, as well as the other instruments as described in this section.

9.1.1 ML/TF/PF/TFS threats

Data from the MBR indicates that in 2022 there were 50,818 active legal persons, with the majority being private limited companies at 48,095. The number of newly registered legal persons has registered a decrease over 2019 to 2022, from a level of 4,266 in 2019 to 2,824 in 2022.

From the active legal persons in 2020, 5,263 had no Maltese involvement except for a registered office, that is, where there is no local presence. In addition, in 2021, from the active legal persons, 5,760 were with no local presence, and in 2022, 6,150 were with no local presence. The number of purpose non-profit foundations as at 2022 amounted to 396 from 361 in 2021.

[47] For the purpose of this document, legal persons refer to commercial partnerships that include Public Limited Liability Companies; Private Limited Liability Companies, Societa Europea, European Economic Interest Grouping, Partnerships *en commandite*, and Partnerships *en nom collectif* as incorporated under the provisions of the Companies Act.

It is to be noted that international incoming requests received by Malta's law enforcement authority in 2021 indicate that the majority of the requests involved legal persons in Malta. Nonetheless, there were no mutual legal assistance received by the Office of the AG and the Malta Police Force with regards to suspicion of BO concealment during the period under review. A number of requests for information as well as spontaneous intelligence reports were received by the FIAU, in which at least one Maltese legal person featured, where some of the Maltese legal persons that featured in these requests had connections with other corporate entities set up in other jurisdictions. The predicate offences identified in these requests for information were mainly in relation to tax crimes, fraud, organised crime, and corruption and bribery. It is again to be noted that the suspicion of concealment of BO was not prevailing in the requests received by the FIAU.

Furthermore, a number of suspicious reports were received by the FIAU from Maltese subject persons, where a smaller share of the reports involved at least one Maltese legal person, and the majority of these reports originated from Maltese credit institutions. When assessing the prevailing predicate offence underlying these suspicious reports, the main offences were tax crimes (specifically corporate income tax and personal income tax), fraud, corruption and bribery, organised crime, and unlicensed licensable activities. Again here, the suspicion of concealment of BO or other similar indicators (such as proposed BO changes after the subject person's requests, BO identification information) was relatively low. The product or service that featured the most in the suspicious reports that involved at least one Maltese legal person, were domestic bank accounts followed by bank accounts in the EU/EEA.

In addition, with regards to arraignments, between 2020 and 2021, 57 legal persons were arraigned, where the discrepancies reported were in relation to a group of six (6) legal persons beneficially owned by the same natural person. Therefore, this data indicates that while incoming requests from foreign jurisdictions and actual cases indicate that the threat of abuse of legal persons related to ML exists, this typically does not include declaration of false or inaccurate BO and the suspected criminals.

In relation to foundations and associations, the threat of abuse for ML purposes can be through the non-disclosure of the existence of the organisation, the identity of all persons involved in the organisation (ownership, if any, and control), its assets and its transactions. Abuse can also be done through the lack of disclosure of the persons involved in the organisation and not only in the setup, but also on a continuing basis. The lack of disclosure of assets, that is, constitutive, accumulating and distributed can also be another means for ML abuse, and this can occur during the lifetime of the foundation.

In line with the above, the following table presents the rating of ML threats for legal persons where the highest ratings prior to assessing the effectiveness of mitigating measures refer to threats of laundering proceeds of crime through schemes using complex structures, schemes involving abandoned commercial partnerships, and incorrect beneficial owner used in ML schemes with tax crime as a predicate offence. As shown in the below table a high threat is in relation to the abandoned legal persons[48]. These are treated as high-risk due to the fact that these might have been used for a one-time transaction which can be ML/TF. There could also be cases where legal persons would be conducting business without any visibility and probably not paying taxes. This

[48] This refers to legal persons that do not submit documents for a considerable number of years.

explains the rating of 'high'. The threat of tax crime due to incorrect BO information is considered to be 'high'. Here it is to be noted that in the national tax risk assessment that was carried out and finalised by December 2021 and also submitted to the FATF, the residual risk of the laundering of foreign tax crime proceeds is mainly driven by the misuse of Maltese legal persons and the use of complex corporate structures, the misuse of the tax refund scheme to launder the proceeds of crimes, the use of cash intensive businesses and the acquisition of immovable property.

Table 13: Rating of ML/TF/PF/TFS threats – legal persons

Threat	Impact	Likelihood	Threat level
ML schemes using complex structures	Severe	Likely	High
ML schemes involving abandoned legal persons (Maltese and Non-Maltese Involvement)	Severe	Likely	High
Incorrect BO used in ML schemes with tax crime as a predicate offence	Severe	Possible	Medium-high
Incorrect BO used in ML scheme with other predicate offences	Significant	Possible	Medium-high
Concealment of BO for ML/TF/PF or TFS	Significant	Possible	Medium-high
ML schemes involving unlicenced financial services	Significant	Possible	Medium-high
Unlawful behaviour in financial markets	Significant	Possible	Medium-high
Use of foundations and associations for ML purposes	Significant	Possible	Medium-High
Illicit use of domestic bank accounts by legal persons with foreign links and complex structures	Significant	Unlikely	Medium

9.1.2 Vulnerabilities

The assessment of the vulnerabilities found an overall rating of the vulnerabilities for the legal persons equivalent to 'medium-high'.

The two main drivers for the vulnerability score are limited financial footprint and complex structures. Both features were analysed by leveraging data from MBR (company data), CBAR (banking information) and National Statistics Office (NACE industry classification) and the following insights were derived:

- A 42% estimate of all legal persons registered in Malta are deemed to be in possession of a Maltese IBAN account
- The likelihood for a legal person with at least one resident shareholder / beneficial owner to have a Maltese IBAN is significantly higher than legal persons without resident beneficial owners, however, this still stands at an estimate of 65%.

Lack of visibility of company activity or in the absence or a limited local footprint has a rating of 'high'. Such legal persons would be expected to have a commercial or other activity going on in Malta, which would in most cases necessitate the opening up of bank accounts to facilitate such an activity. This is in particular so for legal persons that are owned by Maltese residents. Whilst a local company may have legitimate reasons for not having a local financial footprint, this is not typical and is indicative of potential concealment of assets outside of the jurisdiction. In addition,

for those legal persons that do not have a Maltese resident this may be implying that there is the opening of legal persons but the carrying out of banking activity is being done in another jurisdiction. It is important that both subject persons as well as competent authorities are aware and scrutinize such scenarios understanding the rationale behind such a setup. Subject persons dealing with such clients must ensure that economic/commercial activity of the individual/company justifies the added costs of not having a domestic but rather a foreign bank account. This vulnerability is further exacerbated in instances where there is no resident auditor, as there are a number of reasons for why there might be no auditor, for instance:

1. New companies have a timeframe of up to 18 months to file the first accounts and the MBR will only be aware of the appointment of the auditor after the mentioned period.
2. In accordance with the 2013/34/EU (Accounting Directive) which Directive consolidates existing legislation with financial reporting, there are certain thresholds that small companies are exempt from filing auditing accounts with the Registry. Therefore, while these small companies are obliged to file audited accounts with the MTCA they are exempt to file audited accounts with the MBR.
3. Some companies fail to file financial statements.

In fact, this last point leads to another key vulnerability, where there is lack of sufficient data exchange between authorities regarding financial statements of legal persons. The MBR is currently working with the MTCA to monitor those legal persons which never filed tax returns and never asked for any tax refund as this can be indicative of limited or non-existent operations.

Challenges related to legal persons having multiple layered structures and multiple jurisdiction structures is another prominent vulnerability with a rating of 'medium-high'. Complex structures with no clear, reasonable or commercial purpose for such a structure and/or use of structures which render it difficult to determine beneficial ownership are a vulnerability. In Malta, out of the multi-layered legal persons, 31% are two-layered ownership structure, which means a Maltese registered company having body corporates as immediate shareholders that are in turn directly owned by natural persons, and 69% are at least two-layered ownership structure with around half of these having at least one-foreign registered immediate corporate shareholder.

In relation to foundations and associations, a vulnerability exists in relation to administrators, given that as things stand, administrators are regulated only in three (3) cases:

- when there is a private foundation with private beneficiaries, in which case the administrators are MFSA authorised and regulated,
- when there are public benefit and social purposes under the Voluntary Organisations Act where the Commissioner of VOs supervises the sector, and
- professional organisations regulated by professional bodies.

In the remaining cases, administrators are not regulated. Most administrators are not subject persons and have no particular obligations relating to ML but are naturally exposed to risks and personal criminal liability under ordinary law if they participate in it or allow it to occur in an organisation of which they are administrators.

Another vulnerability is in relation to the wide delegation of powers by administrators to third parties who are not holders of the office. This could exploit further the threats of ML if there is lack of supervision or possibly cross border context.

The results of the assessment of the vulnerabilities are shown in the following table.

Table 14: Vulnerabilities – legal persons

Vulnerability	Impact	Exposure	Vulnerability level
Limited financial footprint in Malta	Severe	High	High
Challenges related to legal persons having multiple layered structures and multiple jurisdiction structures	Severe	Moderate	Medium-high
Lack of sufficient data exchange between authorities regarding financial statements of legal persons	Significant	Moderate	Medium-high
Relatively high number of foreign-owned legal persons	Moderate	Moderate	Medium
Level of sufficient understanding how to identify BO in complex situations	Moderate	Moderate	Medium
Relatively large number of legal persons registered in Malta	Moderate	Moderate	Medium
Lack of power by the Authority (MBR) to verify the BO information	Moderate	Low	Medium -Low

9.1.3 Effectiveness of mitigating measures

The overall level of effectiveness of mitigating measures in the legal persons sector is 'high', which is the result of the enhanced efforts that are being done in order to ensure that the BO information on legal persons held by the MBR on its online portal is indeed accurate and up to date. In April 2021 the MBR was recognized as a supervisory authority in terms of the PMLFTR and therefore enhanced measures to complement this new role had to be included. In addition, Malta took various measures to enhance the Registry's approach and to ensure that it offers a well-resourced and proactive company registry holding accurate and up-to-date BO information. The Register is online and available to competent authorities free of charge and also via the Application Interface Program (AIP).

In addition to this, by virtue of Act LX of 2021 Malta transposed Directive (EU) 2019/1151 amending Directive (EU) 2017/1132 as regards the use of digital tools and processes in company law. This directive also delved into the disqualification of directors and Member States were obliged that in order to ensure that all persons interacting with companies or branches are protected and that fraudulent or other abusive behaviour is prevented, it is important that competent authorities in Member States are able to verify whether the person to be appointed as a director is not prohibited from performing the duties of a director. To that end, competent authorities should also know whether the given person is recorded in any of the registers relevant for disqualification of directors in other Member States by means of the system of interconnection of business registers. Since this register is still not available at EU level, Malta is obliging every new director

to provide a self-declaration that he is not disqualified in any other Member State. In addition, the verification of EU resident beneficial ownership will also be enhanced once all the Member States are connected to the Beneficial Ownership Registers Interconnection (BORIS). The MBR, along other three (3) EU Member States, was one of the first countries to be connected to BORIS in 2022.

Moreover, the MBR conducts screening on all involvements of a new proposed company (that is before incorporation stage) and also whenever there are changes in BOs, shareholders, and directors in an existing company. In these cases, the screening is not done on a risk-based approach due to the fact that screening is done in all cases without any exemptions. The same screening takes place also before the Registrar initiates the defunct procedure.

Furthermore, improvements in the FIAU's internal processes to exchange information internally and externally with other national authorities have been instrumental in enhancing the FIAU's risk assessment processes to identify higher risk gatekeepers, potential discrepancies in BO information, and potential breaches of AML/CFT BO-related obligations.

All this led to 'very high' STR reporting by supervisory authorities, a 'very high' level of national cooperation, even with regards to sanction screening carried out by MBR and the other supervisory authorities, and an effective enforcement by supervisory authorities of BO related issues. Moderate improvements are needed with regards to CDD carried out on legal persons' bank account when pooled accounts are used, and with regard to STR reporting by subject persons and the multi-pronged approach[49], given that for example, the multi-pronged approach is missing when legal persons are not set up by a local CSP or not banking in Malta. For example, the percentage of legal persons set up by a CSP stood at 98.3% in 2020, which decreased to 95.4% in 2021, to 91.5% in 2022.

With regards to foundations, it is to be highlighted that foundations can only be set up via notarial public deed and with notaries being subject persons there are due diligence obligations taking place over the founders and administrators, and when the beneficiaries are named and recorded, over the beneficiaries as well as the assets endowed. The notary is responsible to hold originals of the deeds and even archive them under strict notarial laws but that has been further strengthened because foundations must then be registered in a public register within set time limits under the law.

Administrators of private foundations are required to be registered with MFSA to act as administrators. Acting as a possible administrator of a private foundation – though in these cases one does not even have a foundation – is a breach of regulatory law and amounts to a criminal offence under the Trust and Trustees Act. It is rare to come across a foundation which is not registered except in the context of very old foundations, which would in any case imply negative consequences under the law, or religious foundations. It is also to be noted that fiduciary duties of administrators mitigate against negligence and even more so criminal activity. Furthermore, the

[49] The revised Recommendation 24 explicitly requires countries to use a multi-pronged approach, i.e., to use a combination of different mechanisms, for collection of beneficial ownership information to ensure that adequate, accurate and up-to-date information on the beneficial ownership of legal persons is available and can be accessed by the competent authorities in a timely manner. Guidance on Beneficial Ownership of Legal Persons (fatf-gafi.org)

VO Act, has implemented ML preventing duties on ordinary administrators (without making them subject persons). From the MBR perspective, it is also highlighted that there is an evident trend on raising the standard of corporate governance generally in the case of legal organisations of all types which mitigates the risks of delegation.

Furthermore, in foundations, the complexity of the context whether of the testamentary type or commercial structures is so high that they nearly always require the involvement of lawyers, accountants or other professionals who are all subject persons, as without them it would be very difficult to comply with the demanding requirements of the law. Having said that, it must be acknowledged that these are not mandatory.

In 2021, the MBR submitted to the FIAU three (3) suspicious reports in relation to foundations which number decreased to two (2) in 2022. From the associations side, there was only one (1) suspicious report in 2021 and another one (1) in 2022. In 2020 and 2021 there was the rejection of new applications by the Foundations and Associations Unit of ten (10) per year. In 2022, 16 new applications were rejected.

In 2022, the MBR was involved in giving two (2) training sessions to the private sector to enhance the knowledge of the persons working within foundations and associations.

The results of the effectiveness of mitigating measures are presented in the below table.

Table 15: Level of effectiveness of mitigating measures – legal persons

Mitigating measures applied at national level	
Controls applied by supervisory authorities in relation to the registration requirements, quality of the corporate registry and accuracy of BO information, supervision, enforcement, guidance and outreach	Very high
Other external factors impacting the AML/CFT framework in place (e.g., Beneficial Ownership Registers Interconnection (BORIS))	Very high
Mitigating measures by foundations and associations – national data	
Foundations can only be set up via notarial public deed and with notaries being subject persons	High
When there is a private foundation with private beneficiaries, in which case the administrators are MFSA authorised and regulated	High
In cases where, all the administrators are non-resident, a local representative is always required to be appointed and retained at all times	High
Mitigation measures applied by subject persons	
Risk understanding, assessment, and management	Substantial
Customer due diligence related controls	Substantial
Reporting of STRs	Substantial
Resources dedicated to AML/CFT and staff knowledge (including MLROs)	High

9.1.4 Residual risk rating analysis

The residual risk ratings are presented in the below table. The overall residual risk of the legal persons that are registered in Malta is equal to 'medium-high' driven by the higher weighting

attributed to no sufficient links to Malta (i.e., when there is no Maltese resident director, totally owned by foreigners, or no Maltese auditor).

Table 16: Residual risk rating – legal persons

Topic	Inherent risk	Effectiveness of mitigating measures	Residual risk	Overall residual risk level
Abuse of Maltese registered legal persons with no sufficient links to Malta, for ML or concealment of BO (i.e., when there is no Maltese resident director, totally owned by foreigners, or no Maltese auditor)	High	Substantial	Medium-high	**Overall residual risk = Medium-high**
Anomalies complex ownership/control structures	Medium-high	Substantial	Medium-high	
Multi-jurisdiction splitting	Medium-high	Substantial	Medium-high	
Abandoned legal persons (Maltese and non-Maltese involvement)	High	Very high	Medium	
Incorrect BO information and concealment of BO	Medium-high	High	Medium	
Establishment of legal persons without the involvement of subject persons	Medium	Substantial	Medium	
Registered legal persons and conducting unlicenced Financial Services	Medium	High	Medium-low	
Illicit use of domestic bank accounts by legal persons	Medium	High	Medium-low	
Use of foundations and associations for ML purposes	Medium	High	Medium-low	

The residual risk is mainly driven by the risk in relation to the abuse of Maltese registered legal persons with no sufficient links to Malta, the misuse of foreign ownership/control, anomalies complex ownership/control structures, and multi-jurisdiction splitting. This reflects the misuse of Maltese registered legal persons, and the use of overly complex corporate structures. Only a small proportion of foreign owned and high-risk legal persons have an IBAN account in Malta which when considering the tight controls applied by banks to legal persons leads to the conclusion that the risk of abuse of the Maltese financial systems through the use of legal persons is limited. Nonetheless, foreign owned and high-risk legal persons are serviced by CSPs and accountants/auditors, which judging by the level of suspicious report detection and supervisory experiences, further improvement is necessary to lower the residual risk of misuse of legal persons for foreign tax crime purposes. The recent fitness and propriety regime for all CSPs introduced by the MFSA are already contributing to boost the compliance culture of CSPs. Concealment of beneficial ownership is not considered to constitute a significant typology in which legal persons may be misused to launder foreign proceeds of crime in Malta.

9.1.5 Recommendations

This section presents a number of recommendations to guide subject persons when applying preventative measures on a risk-based approach.

Ensuring risk awareness by subject persons
As recommended by the EU SNRA (2022)[50], ensure that subject persons are aware of risks associated with legal persons, particularly in the context of non-face to face business relationships, and when dealing with non-EU legal persons and require that in those cases subject persons pay particular attention to the corporate structure of the client to ascertain who ultimately owns or controls it.

Align the business risk assessment and the customer risk assessment with the results of the NRA and periodically update the customer risk profiles.
Review regularly the risk assessment and management processes, taking into account the contextual environment within which the activity being carried out is.

Update the customer due diligence and enhanced customer due diligence, including transaction monitoring, in line with the findings of the NRA.
Adopt due diligence measures that are commensurate with the risks, thus adopting a risk-based approach that should allow banks to be more flexible in their application of customer due diligence measures in case of lower ML/TF risks and thereby contributing to greater transparency and traceability of financial flows.

Implement risk-based customer due diligence policies, procedures and processes.

Ensure that there are adequate screening procedures

Review the effectiveness of monitoring systems
Monitoring should be carried out on a continuous basis and commensurate with the risk assessment.

Verification procedures of customers
While obtaining an organigram from customers to explain the ownership and control structure of the customer is a good starting point for the purpose of establishing the link between the customer and the BO/s, this procedure cannot be taken to be an independent verification measure. Therefore, CSPs should subsequently conduct independent research to verify the information on the structure chart. This can be done by consulting online commercial databases, company registries, relevant audited accounts or by obtaining certification by any of the persons referred under Section 4.3.1.2(i)(b) of the Implementing Procedures.[51]

Senior managing official
Recognising the senior managing official as the BO of the customer in terms of Tier 3 should only be resorted to after exhausting all possible means to identify a BO in accordance with Tier 1 and

[50] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52022SC0344&from=EN p. 152
[51] Compliance-With-beneficial-Ownership-Obligations-by-CSPs.pdf (fiaumalta.org)

Tier 2 and if there are no grounds of suspicion. A record of the actions taken to try to identify a BO in terms of Tier 1 and Tier 2 should be retained by the CSP as part of its recording keeping obligations and certification by any of the persons referred under Section 4.3.1.2(i)(b) of the Implementing Procedures.

Written procedures

CSPs need to ensure that their written procedures define which sources meet the criteria of 'independent' and 'reliable' when obtaining identity verification documentation and ensure that officers and employees are aware of these procedures. All BO identity details as per Section 4.3.1 (i) of the Implementing Procedures should be verified, although in low-risk situations, the BO's official full name, date of birth and permanent residential address can suffice.

9.2 Legal arrangements

This section presents the findings of the risk assessment on legal arrangements. The European Commission (2021) defines 'legal arrangement' as an express trust or an arrangement which has a similar structure or function to an express trust, including *fiducie* and certain types of Treuhand and *fideicomiso*. FATF defines an express trust as *"a trust clearly created by the settlor, usually in the form of a document, e.g., a written deed of trust. They are to be contrasted with trusts which come into being through the operation of the law and which do not result from the clear intent or decision of a settlor to create a trust or similar legal arrangements (e.g., constructive trust)."*

The relevant parties and elements to this sector in line with the Trust and Trustees Act[52], are the:

- ***Settlor***: the person who creates the trust and includes a person who provides trust property or makes a disposition on trust or to a trust,
- ***Trustee***: the person or persons holding the property or in whom the property is vested in terms of the trust agreement and in accordance with the provisions of Maltese law, and
- ***Beneficiary***: a person entitled to benefit under a trust or in whose favour a discretion to distribute property held in trust maybe exercised.

The total number of trusts reported on TUBOR in May 2022, amounted to 3,486. This figure comprises both Maltese trusts (trusts which are governed by Maltese law as their proper law) and foreign trusts (trusts which are governed by non-Maltese law as their proper law).

Subject persons are to assess their risks not only based on the analysis in their respective sectoral section, but also on additional sections, such as, the overall ML risks 'section 11', 'section 12' that presents the TF risks, 'section 13' on PF and TFS related risks, as well as the other instruments as described in this section.

9.2.1 ML/TF/PF/TFS threats

Data from TUBOR for 2021 indicates that the average amount of trusts reported by trustees amounts to 30.8 trusts per trustee. There are a total of 83 trustees which are deemed to be administering a minimum concentration of trusts, as they are administering 10 trusts or less. There are a total of 24 trustees which are deemed to be administering a medium concentration of trusts, which implies administering 11-50 trusts. There are a total of six (6) trustees which are deemed to administer the maximum concentration of trusts, that is, administering more than 51 trusts. To note that in this category there is one (1) trustee that administers 1,911 trusts, however it should be noted that almost 50% of these trusts are retirement schemes set up as trusts, which would also be licensed in their own right and are therefore subject to regulation in terms of the applicable law.

In assessing the threats through the misuse of trusts, the assessment took into consideration the data on the nationality and residence of the settlors and the beneficiaries. The analysis of the granular data indicated that 11.8% of the individual settlors registered on TUBOR are Maltese nationals, and 12.8% of the individual settlors reside in Malta. With regards to the legal persons, 52.6% were registered in Malta. When assessing the nationality of all individual settlors reported

[52] LEĠIŻLAZZJONI MALTA (legislation.mt)

on TUBOR in terms of EU and non-EU nationality, it was found that a significant share of the non-EU nationals originated from the UK with 63.3%, followed by Malta with 11.8%, and Italy with 4.4%. The analysis indicates that the threat here is contained given the low percentage share accounted for by the high-risk countries. Furthermore, the analysis revealed that although there is a higher percentage share of settlors residing in higher risk jurisdictions, as opposed to settlors having a nationality from higher risk jurisdictions, the percentages are relatively low.

When assessing the legal persons' settlors' country of registration, the majority of the reported legal persons' settlors' country of registration is in the EU with a share of 62%, where Malta accounts for a share of 52.6%.

In relation to the beneficiaries, 11.8% of the individual beneficiaries are Maltese nationals, and 12.5% of the individual beneficiaries reside in Malta. With regards to the legal persons, 17.6% were registered in Malta. Even with beneficiaries, the threat here is limited in view of the low percentage share accounted for by the high-risk countries. Additional data shows that the beneficiaries on the trusts that are administered by non-EU legal person trustees or co-trustees do not reside in high-risk countries.

In addition, there was a minimal number of exchanges of information requests received by the MTCA between 2019 and 2021.

Further to the analysis made, the following table presents the rating of threats for the legal arrangements.

Table 17: Rating of threats – legal arrangements

Threat	Impact	Likelihood	Threat level
Abuse of trust structures for concealment of beneficiaries for ML	Significant	Possible	Medium-high
Abuse of trusts to enable the enjoyment of use of laundered funds including prevention of their confiscation	Significant	Possible	Medium-high
Abuse of trust structures for foreign tax crime purposes	Significant	Possible	Medium-high
Illicit funds settled in the trust	Significant	Unlikely	Medium
Abuse of trust structures for concealment of beneficiaries for TF, PF or sanction evading	Significant	Unlikely	Medium
Abuse of trust structures for domestic tax crime purposes	Significant	Unlikely	Medium

9.2.2 Vulnerabilities

The EU SNRA (2022) presents as a vulnerability the fact that *"the complex structure of trusts makes the identification of the beneficial owners difficult and requires further efforts to determine the true nature of the trust relationship"*.[53] In assessing vulnerabilities in legal arrangements, the

[53] FAFT and Egmont Group (July 2018), Concealment of Beneficial Ownership.

factors that are taken into consideration are trusts' attractiveness for non-residents, the limited information on the type of assets managed by trustees and their location, the difficulty in ascertaining the source of funds/source of wealth when the settlor is from non-EU jurisdiction, the difficulty in ascertaining the accuracy of statements as to beneficiaries residing in non-EU countries, the volume of assets controlled by trustees, and the lack of sufficient understanding of legal arrangements by competent authorities.

The MBR is an added layer of supervision in the incorporation of the legal person reported as settlor on TUBOR. With Maltese registered legal persons, the MBR would also require the BO of the said Maltese legal person to be reported in the MBR register of beneficial owners of companies and other legal persons falling within its remit, and therefore the data would be available to competent authorities from the said register. Similarly, where the legal person settlor is a company which is registered in an EU Member state, the BO information thereof should be reported in the BO register of companies of such member state, and therefore eventually available to all competent authorities via the interconnection of BO registers required by the 5th AMLD. However, to note that in relation to some other jurisdictions, there might be a vulnerability since the BO of the foreign legal person settlor may not be easily or properly ascertainable. In fact, understanding of the BO specifically in the context of foreign ownership presents a vulnerability as this introduces issues in relation to transparency, oversight and enforcement, particularly with non-cooperative jurisdictions. An added vulnerability here is the inability to monitor what is happening in non-EU countries due to the inability to ascertain beneficiaries in non-EU countries.

Table 18: Rating of the vulnerabilities – legal arrangements

Vulnerability	Impact	Exposure	Vulnerability level
Limited information on the type of assets managed by trustees and their location	Significant	High	Medium-high
Difficulty in ascertaining the source of funds/ source of wealth when the settlor is from non-EU jurisdiction[54]	Severe	Moderate	Medium-high
Difficulty in ascertaining the accuracy of statements as to beneficiaries residing in non-EU countries	Significant	Moderate	Medium-high
Lack of sufficient understanding of legal arrangements by competent authorities	Significant	Moderate	Medium-high
Volume of assets controlled by trustees	Significant	Moderately low	Medium

[54] In most cases where a trust is being newly set up, it is the licensed trustee who is involved in such set up and required to abide by the customer due diligence procedures (including identification and verification of the settlor, and his SoW/SoF) vis-à-vis the trust structure. It should also be noted that licensed entities under the Trusts and Trustees Act can provide CSP services in terms of the regulatory framework but are required to notify the Authority of this. The MFSA takes this into consideration in its supervisory work. On the other hand, a CSP cannot provide any of the services regulated by the Trusts and Trustees Act and if they wish to provide such services, they would be required to apply for authorisation under the said Act.

9.2.3 Effectiveness of mitigating measures

The 2018 NRA rated the effectiveness of mitigating measures for the legal arrangements as 'low'. There were AML/CFT controls in place for trusts, but these were deemed to provide a relatively low level of mitigation of inherent risk. This was largely caused by challenges in market entry controls and ongoing monitoring. TUBOR, an online register that has been in place since June 2018, at the time was fully populated with the BO information of all trusts which generate tax consequences (in line with the 4th AML Directive). However, with legislative amendments enacted in February 2020 (following transposition of the 5th AML Directive), the register now also includes information for all trusts which were previously not captured, amounting to a total of 3,486 reported trusts, as at May 2022. The trusts for which BO is reported include both Maltese trusts (governed by Maltese law) and foreign trusts (governed by non-Maltese law) as the requirement to report BO information of trusts applies to all licensed trustees in Malta, irrespective of the governing law of the trust. Moreover, since trustees in Malta are subject persons, they are required to carry out due diligence and identify and verify the identity of all beneficiaries, irrespective of whether such beneficiaries are Maltese or foreign. In addition, some of the trusts reported also include trusts administered by non-EU trustees where such trustee established a business relationship in Malta, as required in terms of the 5th AML Directive.

Since 2020, the MFSA incorporated consideration of AML/CFT/Financial Crime within its authorisations processes and supervisory interactions in what is referred to as the MFSA's AML Integration Exercise. The MFSA has, in the course of its supervision, come across situations and trusts where it was deemed that a settlor was involved heavily in the administration of the trust assets, and therefore the effective divestment of ownership and control by the settlor was brought into question. In such cases the MFSA investigates the circumstances and in case of serious findings takes enforcement action, including through the imposition of administrative penalties, and, in a particular case, the MFSA restricted the licence of the trustee in question. Here licensed trustees would also be directed to take remedial action to ensure that the settlor does not interfere unnecessarily in the administration of the trust, and the trustee was required to provide evidence that decisions were being taken by the trustee in terms of the trust instrument. These cases would be followed through follow up inspections.

Taking into account the national controls and the controls by the sector, the level of effectiveness of mitigating measures is as follows:

Table 19: Effectiveness of mitigating measures – legal arrangements

Mitigating measures applied at national level	
Controls applied by Supervisory Authorities in relation to the registration requirements, quality of the corporate registry and accuracy of BO information, supervision, enforcement, guidance and outreach	Very high
Mitigation measures applied by subject persons	
Risk understanding, assessment and management	Substantial
Customer due diligence related controls	Substantial
Reporting of STRs	Substantial
Resources dedicated to AML/CFT and staff knowledge (including MLROs)	High

The overall level of effectiveness is 'high' and minor improvements are needed with regards to licensing and authority, the enforcement actions by supervisory authorities, guidance and outreach, and the commitment by the subject persons towards ensuring remediation of breaches. On the other hand, substantial improvements are needed on the risk understanding and assessment that will in turn lead to enhanced quality and quantity of reported STRs by trustees. Minor improvements are needed in relation to the AML/CFT framework in place.

9.2.4 Residual risk analysis

As shown in the below table, the overall risk rating for abuse of trust structures for ML/TF purposes is 'medium' and is mainly driven by the risk of abuse for concealment of beneficiaries for ML, the threat of abuse of trusts to enable the enjoyment of use of laundered funds including prevention of their confiscation, and the abuse of trust structures for foreign tax crime purposes.

Table 20: Residual risk analysis – legal arrangements

Topic	Inherent risk	Effectiveness of mitigating measures	Residual risk	Overall sectoral residual risk
Abuse of trusts for concealment of beneficiaries for ML	Medium-high	Substantial	Medium-high	**Overall residual risk of the sector = Medium**
Abuse of trusts to enable the enjoyment of use of laundered funds including prevention of their confiscation	Medium-high	Substantial	Medium-high	
Abuse of trust structures for foreign tax crime purposes	Medium-high	Substantial	Medium-high	
Illicit funds settled in a trust	Medium	Substantial	Medium	
Abuse of trust structures for concealment of beneficiaries for TF, PF, or sanction evading	Medium	High	Medium-low	
Abuse of trusts for domestic tax crime purposes	Medium	High	Medium-low	

9.2.5 Recommendations

This section presents a number of recommendations to guide subject persons when applying preventative measures on a risk-based approach.

Align the business risk assessment and the customer risk assessment with the results of the NRA and periodically update the customer risk profiles.
Review regularly the risk assessment and management processes, taking into account the contextual environment within which the activity being carried out is.

Update the customer due diligence and enhanced customer due diligence, including transaction monitoring, in line with the findings of the NRA.

Adopt due diligence measures that are commensurate with the risks, thus adopting a risk-based approach that should allow banks to be more flexible in their application of customer due diligence measures in case of lower ML/TF risks and thereby contributing to greater transparency and traceability of financial flows. Furthermore, more emphasis should be made on the identification and verification of the source of wealth / source of funds of the settlors (in particular those who are non-EU/EEA).

Implement risk-based customer due diligence policies, procedures, and processes.

Review the effectiveness of monitoring procedures
Monitoring should be carried out on a continuous basis and commensurate with the risk assessment and thus increasing the frequency monitoring in case of any increase in risk rating during the course of business relationships.

9.3 Citizenship and residency by investment schemes

Malta has in place a citizenship by investment (CBI) scheme and a residency by investment (RBI) scheme. Malta's CBI scheme, known as Citizenship by Naturalisation for Exceptional Services by Direct Investment, is administered by Agenzija Komunita Malta (or Community Malta Agency), which was established in November 2020. The new agency was established taking into account recommendations put forward by the European Commission and replaced the Malta Individual Investor Programme Agency (MIIPA) which was responsible for managing the Malta Individual Investor Programme (or the IIP). MIIPA had stopped receiving new applications in August 2020 and was subsequently closed.

As part of the application process under the IIP, applicants were required to invest in Government Bonds, equities or funds listed on the Malta Stock Exchange. Between 2014 to 2021, such investments totalled €221.3 million. Under the new framework regarding the acquisition of citizenship by investment launched at the end of the year 2020 there is no such requirement.

The RBI scheme, known as the Malta Permanent Residence Programme (MPRP) is a straightforward residency-by-investment programme based on investments in property and government contributions. It is administered by Residency Malta Agency. Launched in 2021, the MPRP replaced the former RBI programme known as the Malta Residence and Visa Programme (MRVP). Under the MRVP programme, applicants were required to invest in Government Bonds, equities or funds listed on the Malta Stock Exchange. Between 2016 and 2022, the equivalent of €379.3 million were invested by MRVP applicants. The new programme launched in 2021 does not have this requirement.

Subject persons are to assess their risks not only based on the analysis in their respective sectoral section, but also on additional sections, such as, the overall ML risks 'section 11', 'section 12' that presents the TF risks, 'section 13' on PF and TFS related risks, as well as the other instruments as described in this section.

9.3.1 ML/TF threats

The threat of abuse by either the citizenship or residency schemes to launder the proceeds of crime is assessed to be through the:

- Laundering through the acquisition of immovable property in Malta
- Abuse of the banking system in Malta
- Abuse of the schemes in order to gain citizenship and residency and set-up a company in Malta
- Abuse of the schemes for potential circumvention of the Common Reporting Standard thus tax crime

Applicants are required to purchase or lease a property in Malta, the value of which depends on the program and area chosen. Data for both the citizenship and the residency schemes indicates that the majority of the successful applicants opted to lease rather than purchase property.

Another threat considered in this sector is the possible abuse of the financial system in Malta to launder proceeds of crime. However, data from the CBAR indicates that only a very minor share

of the approved applicants in both the citizenship and the residency schemes have a Maltese IBAN account in their name, or in the name of a legal person beneficially owned by them. This, amalgamated with the previous finding, supports the view that the threat of illicit foreign funds being laundered in Malta by persons benefitting from Maltese CBI/RBI schemes is 'medium', as shown in the below table.

Another threat assessed in relation Malta's CBI/RBI schemes is in relation to the possible abuse of Maltese legal persons by individuals benefitting from Malta's CBI/RBI. Data available to the authorities supports the conclusion that such threat is significant and possible taking into account that from the newly registered legal persons in Malta in 2021, 3% of newly registered legal persons are BOs that are approved applicants of the CBI scheme.

Furthermore, another potential threat of laundering funds and movement of funds for TF would be through legal arrangements. Here, by cross-checking with the TUBOR data, in 2021, 8% of the approved CBI applicants appear as settlors or beneficiaries in eight (8) trusts on TUBOR (some individuals feature in the same trust structure), with the nationality form some high-risk jurisdictions. In addition, another three (3) individuals of the approved applicants of the CBI scheme for 2021 also featured in TUBOR's historical data for three (3) other trusts as settlor and/or beneficiary, which however are no longer reported on TUBOR since one (1) of the trusts has been terminated, whereas the other two (2) trusts have been transferred to a trustee outside of Malta.

With regards to the RBI scheme, out of the total approved applicants from 2016 to 2022, only two (2) individuals feature as settlor and/or beneficiary in two (2) different trusts, with the nationality and residency of one being from a high-risk jurisdiction. Another two (2) individuals also featured in TUBOR's historical data for two (2) other trusts, as settlor and/or beneficiary, however these two (2) trusts are no longer reported on TUBOR since both trusts have now been terminated.

The MPF has three (3) investigations concerning the citizenship and residency by investment schemes. Two (2) of these investigations are now closed, one of which resulted in a prosecution, and the other archived as the investigation concluded that no crime was committed.

The number of cases in which a suspicion of ML/TF was identified by the Agenzija Komunita Malta and Residency Malta Agency is particularly low. In terms of the citizenship schemes, during the period from 2018 – 2022 there were 367 refusals out of which 37 were refused on the basis of ML/TF suspicions or concerns and were subsequently reported to the FIAU. The following table shows the rating of the ML/TF threats for both the residency and the citizenship schemes.

Table 21: Rating of ML/TF threats - Citizenship and Residency by investment schemes

Threat	Impact	Likelihood	Threat level
Abuse of RBI/CBI for laundering through multi-jurisdictional schemes:			
of foreign proceeds of crime through the acquisition/leasing of immovable property in Malta	Significant	Possible	Medium-high
of foreign proceeds of crime through investments in financial assets in Malta	Significant	Possible	Medium-high
through legal persons and legal arrangements	Significant	Possible	Medium-high
the proceeds of foreign tax crime	Significant	Possible	Medium-high
through the banking system in Malta	Significant	Unlikely	Medium

9.3.2 Vulnerabilities

The vulnerabilities assessed in this sector were mainly that:

- In themselves, the nature of the schemes, involve high net worth individuals who are oftentimes coming from jurisdictions that present higher ML/TF risks, and at time who may also be PEPs. This creates challenges in terms of customer due diligence, particularly in establishing their source of wealth. For instance, in 2018, 17% of the successful applicants were PEPs. The equivalent figure decreased to 9% in 2020. It is to be noted that in 2022 the Maltese government has suspended its citizenship scheme for Russian and Belarusian citizens.
- The possible reliance by subject persons on agents processing CBI/RBI applications, of those granted citizenship is a potential vulnerability.
- The fact that, in some cases, applicants originate from jurisdictions the Financial Intelligence Units which are not members of the Egmont Group of Financial Intelligence Units has been identified as another vulnerability.

The following table presents the ratings of the assessment of the vulnerabilities.

Table 22: Vulnerabilities - Citizenship and Residency by investment schemes

Vulnerability	Impact	Exposure	Vulnerability level
Performing CDD on applicants from high-risk countries	Significant	Very high	High
Performing CDD for applicants who are PEPs	Significant	High	Medium-high
International cooperation vulnerabilities	Significant	Moderate	Medium-high
The reliance by agents and subject persons on the granting of the citizenship	Significant	Moderate	Medium-high

9.3.3 Effectiveness of mitigating measures

Overall, there are several mitigating measures in place that are considered to provide a high degree of effectiveness in mitigating the ML/TF risks posed by CBI/RBI schemes. Both schemes have a high refusal rate and the respective agencies responsible for administering these schemes have implemented rigorous controls. In addition to these measures, the AML/CFT controls applied by various categories of subject persons servicing applicants of any of the schemes, such as the notarial sector and the financial institution/banking sectors, also contribute to the overall mitigating measures.

Furthermore, an enhanced level of cooperation between the FIAU and Agenzija Komunita Malta and Residency Malta Agency takes place on an ongoing basis. The FIAU receives information on all applicants at application stage in a timely manner so as to be able to carry out a series of checks during application stage. In addition, sharing of information mechanisms have also been put in place between the intelligence analysis section and supervision section of the FIAU in cases where client due diligence weaknesses are noted in subject persons that are agents in terms of the CBI/RBI programmes.

Furthermore, it is also to be noted that Malta has given a commitment under the EU Recovery and Resilience Plan in relation to the exchange of information relating to successful applicants going forward as from the first quarter of 2022.

Moreover, the FIAU Implementing Procedures (which are legally binding) require subject persons to know whether their clients benefit from any citizenship by investment schemes (even if not Malta's scheme), and to consider such customers as posing a higher risk of ML/TF and to be subjected to enhanced customer due diligence. Subject persons cannot rely on any checks carried out by the agency responsible for the scheme but are required to carry out their own due diligence measures. Furthermore, it is to be noted as well that the FIAU Implementing Procedures set clear expectations on the need to carry out enhanced scrutiny when dealing with complex structures – which may be present in relationships when dealing with persons benefiting from citizenship schemes.

As part of its risk-assessment process (through the REQs and CASPAR), the FIAU obtains information to understand a subject person's risk exposure to high-net worth individuals and uses this information when preparing its supervisory plan. Prior to carrying out a compliance examination, the FIAU also asks subject persons to provide client lists, which would also enable the FIAU to include, in its sampling, customers who benefit from CBI/RBI programmes.

The CBI/RBI schemes in Malta require all applicants to provide information regarding their Tax Identification Number (TIN) and are also informed that this information will be forwarded to the MTCA when they acquire citizenship. Such measures started to be implemented as from 2022.

Furthermore, the Common Reporting Standard (CRS) (and the US Foreign Account Tax Compliance Act, FATCA) applies to all those jurisdictions where Malta has an arrangement to exchange information automatically. This means that such exchange may be had with 81 jurisdictions (54 non-EU jurisdictions and 26 EU Member States and the US).

Nationals from sanctioned countries or who have close ties with sanctioned countries, are ineligible. At the time of writing, these countries included Afghanistan, North Korea, Iran, Democratic Republic of Congo, Somalia, South Sudan, Sudan, Syria, Yemen and Venezuela. Additionally, applications from the Russian Federation and the Republic of Belarus are currently not eligible.

2021 FIAU REQ data indicates that banking services are being offered to approximately only 650 customers benefitting from such schemes, most of which were onboarded prior to 2019. Since (and including) 2019, less than five (5) customers per year were onboarded by banks licenced in Malta, indicating that domestic banks have become more risk averse and less keen to onboard customers benefitting from CBI/RBI schemes. Further statistics also indicate that banks have also de-risked by way of terminating relationships with existing clients who benefit from CBI/RBI schemes.

Given the above key findings, the ratings are presented in the following table:

Table 23: Effectiveness of mitigating measures - Citizenship and Residency by investment schemes

Mitigating measures applied at national level	
Controls applied by agencies and the supervisory authorities in relation to the applicants, supervision, enforcement, guidance and outreach	Very high
International cooperation	Substantial
Mitigation measures applied by subject persons	
Risk understanding, assessment and management	High
Customer due diligence related controls	High
Reporting of STRs	High
Resources dedicated to AML/CFT and staff knowledge (including MLROs)	High

The overall level of effectiveness is 'high' and minor improvements are needed with regards to the mitigating measures by Agenzija Komunita' Malta and the Residency Malta Agency. Moderate improvements are needed with regards to the exchange of tax information with MTCA[55], and the exchange of information with international counterparts, and additional outreach by the FIAU.

9.3.4 Residual risk analysis

The analysis revealed that the exposure of Malta's financial system to persons who are benefiting from Malta's CBI/RBI schemes is somewhat limited, thereby reducing the risk of having the laundering of funds or the movement of funds for TF through the domestic financial system. The acquisition and/or leasing of property by individuals granted citizenship under the Maltese Citizenship Scheme is on the decline. In addition, the mitigating measures in place are of a 'high' nature thereby leading to an overall residual risk for abuse of these schemes being 'medium'.

[55] Despite the fact that there is increased exchange of information it is to be noted that not all countries that are granted citizenship or residency actually form part of the Common Reporting Scheme.

Table 24: Residual risk analysis – Citizenship and Residency by investment schemes

Topic	Inherent risk	Effectiveness of mitigating measures	Residual risk	Overall residual risk level
Abuse of RBI/CBI for laundering through multi-jurisdictional schemes:				
of foreign proceeds of crime through the acquisition/leasing of immovable property in Malta	Medium-high	High	Medium	**Overall residual risk = Medium**
of foreign proceeds of crime through investments in financial assets in Malta	Medium-high	High	Medium	
through legal persons and legal arrangements	Medium-high	High	Medium	
the proceeds of foreign tax crime	Medium-high	High	Medium	
through the banking system in Malta	Medium	High	Medium-low	

9.3.5 Recommendations

This section lists key recommendations for subject persons that have been identified during the risk assessment, the implementation of which will improve the sector's resilience to abuse from ML/TF and close the gap in identified threats and/or vulnerabilities.

As part of their customer risk assessment procedures, subject persons are encouraged to ensure that, prior to onboarding a customer, they assess whether a potential customer is a candidate/beneficiary of CBI/RBI schemers and apply enhanced due diligence measures in accordance with the level of risk posed by that potential customer.

Subject persons are also encouraged to carry out robust checks on source of wealth/source of funds, particularly when carrying out higher risk transactions, on behalf of customers benefitting from such schemes, and be alert for possible red flags, such as tax crime, corruption or sanctions evading.

9.4 Voluntary Organisations (non-profit organisations)

This section presents the results of the Voluntary Organisations (VOs) or the non-profit organisations' (NPOs) risk assessment where the focus is on assessing the VOs (NPOs) that fall within the FATF scope risk, that is: *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".*[56] Against this definition, as at June 2022, out of the 1,708 enrolled VOs (NPOs) with the OCVO, 55 VOs (NPOs) fall within the FATF scope.

Subject persons are to assess their risks not only based on the analysis in their respective sectoral section, but also on additional sections, such as, the overall ML risks 'section 11', 'section 12' that presents the TF risks, 'section 13' on PF and TFS related risks, as well as the other instruments as described in this section.

It is also to be noted that the list of high-risk jurisdictions covered in this risk assessment is wider than the list adopted under the TF risk assessment. For the VO (NPO) sector, the list encompasses the socio-politico-economic situation of the countries, geopolitical analysis and research based on the:

- Institute for Economics and Peace Global Terrorism Index 2020[57];
- US Government Country Reports on Terrorism 2019 Bureau of Counter-Terrorist[58],
- the EU Delegated (EU) 2016/1675[59] and
- the EU Sanctions Map.[60]

9.4.1 ML/TF threats

Out of the enrolled VOs (NPOs) with the OCVO, only 3% of the enrolled VOs (NPOs) fall under the scope of FATF recommendation 8, where these VOs (NPOs)were categorised in terms of their annual income, the activities carried out by the VO, and the jurisdictions within which the VO (NPO) operates and has partners. According to this further categorisation, out of the category that generates the highest revenue (that exceeding €250,000), there are only ten (10) VOs (NPOs). Furthermore, out of the 55 VOs (NPOs) that fall under the scope of the FATF recommendation 8:

- only 35 disbursed funds to high-risk jurisdictions

Additionally, out of these 55 VOs (NPOs):

- 33 have as their scope of work international development and humanitarian aid,

[56] FATF (2015), Best Practices, Combating the Abuse of Non-Profit Organisations, (Recommendation 8).
[57] https://visionofhumanity.org/wp-content/uploads/2020/11/GTI-2020-web-1.pdf
[58] https://www.state.gov/wp-content/uploads/2020/06/Country-Reports-on-Terrorism-2019-2.pdf
[59] https://eur-lex.europa.eu/eli/reg_del/2020/855/oj
[60] https://www.sanctionsmap.eu/

- 13 are ethnic based organisations and
- only one (1) organisation addresses diaspora groups.

In 2020, all the 1,708 enrolled VOs (NPOs) spent €98 million. Out of this amount, 7% was disbursed by the 35 VOs that disbursed funds to high-risk jurisdictions. The category that generates the highest revenue and income, that captures ten (10) VOs (NPOs), disbursed 94% of this 7% to high-risk jurisdictions. It is also to be noted that, of this 7% disbursed to high-risk jurisdictions:
- 31.8% of the disbursed funds were from one VO (NPO)
- 18.7% by another VO (NPO)
- 17.97% by another VO (NPO)
- 3.6% by the remaining VOs (NPOs)

In comparison, in 2021, 36 VOs (NPOs) disbursed €9.5 million to 50 high-risk jurisdictions (statistics as on the 29 June 2022) as compared to €7 million disbursed in 2020.

Between 2019 – January 2022 the FIAU received 15 suspicious reports that involved a Maltese VO (NPO). Out of these 15 Reports only three (3) were submitted in view of terrorism related indicators. These were submitted by the OCVO, and the analysis of which has been concluded and did not lead to any dissemination.

In view of the above key findings, the results of the ratings are presented in Table 25.

Table 25: Rating of ML/TF threats – VOs (NPOs)

Threat	Impact	Likelihood	Threat level
Threat of TF abuse through raising of donations in Malta	Severe	Possible	Medium-high
TF threat of disbursement of funds by VO (NPO) including to high-risk jurisdictions	Severe	Possible	Medium-high
Threats of ML/TF abuse of the VO (NPO) related to the composition of their administrators and other staff	Significant	Unlikely	Medium
Threat of ML related to misappropriation or mismanagement of VOs (NPOs) expenditures	Significant	Unlikely	Medium
Threat of abuse of VOs (NPOs) for ML (including VOs (NPOs) related to sports)	Significant	Unlikely	Medium
Funding of VOs (NPOs) for use of terrorist acts in Malta	Significant	Very unlikely	Medium

9.4.2 Vulnerabilities

As shown in the table hereunder, the VO (NPO) sector recorded an overall 'medium' in terms of vulnerabilities. This is mainly driven by the vulnerability in terms of the issue that no administrative penalties are available for this sector and with reference to the general vulnerability on the constitutionality of sanctions. The other 'medium-high' vulnerability relates to the lack of ML/TF risk awareness among the VOs (NPOs).

Another important vulnerability is in relation to the lack of access to the financial system, which is related to the issue of de-risking. This is rated as 'medium' in view of the fact that with regards to the 55 VOs (NPOs) that fall under the FATF scope, 41 out of 55 VOs (NPOs) have a bank account. However, when assessing all the enrolled VOs (NPOs) including those that do not fall under the FATF scope, then it follows that in line with data from CBAR, as at December 2021, 67% of all the VOs (NPOs) registered with the OCVO hold accounts with Maltese licensed credit/financial institutions.

The resulting risk ratings are as follows:

Table 26: Rating of vulnerabilities – VOs (NPOs)

Vulnerability	Impact	Exposure	Vulnerability level
Effective, proportionate, and dissuasive sanctions	Significant	Moderate	Medium-high
Lack of ML/TF risk awareness among the VOs (NPOs)	Severe	Moderate	Medium-high
De-risking of some of the VOs (NPOs) by credit institutions	Significant	Moderately low	Medium
Some VOs (NPOs) set up without the involvement of subject persons	Significant	Moderately low	Medium
Degree of cross-border exposure of VO (NPO) activity	Severe	Moderately low	Medium
Use of (unregulated) crowdfunding platforms by VOs (NPOs)	Severe	Moderately low	Medium

9.4.3 Effectiveness of mitigating measures

This section presents the ratings of the effectiveness of mitigating measures taking into consideration both the national controls as well as the controls by the subject persons. It is pertinent to point out, that the disbursement to high-risk jurisdictions by the 36 VOs (NPOs) were all made via bank transfers. Furthermore, out of the 36 VOs (NPOs) that disbursed funds to jurisdictions within or near those areas that are most exposed to terrorist activity, 21 have the involvement of a subject person in their set-up.

On average, the level of effectiveness of mitigating measures is 'substantial', where major improvements are required on the risk-based supervision by OCVO regarding program planning and monitoring including VO (NPO) local partners in high-risk jurisdictions. Moderate improvements are required with regards to outreach by OCVO to the high-risk VOs (NPOs). On the other hand, minor improvements are needed on the OCVO risk-based due diligence of VOs (NPOs), the national cooperation and information exchange regarding VOs (NPOs), and mitigating measures by subject persons of their VO (NPO) clients.

Table 27: Effectiveness of mitigating measures – VOs (NPOs)

Mitigating measures by the regulatory authorities	
Controls applied by the supervisory authorities in relation to the applicants, supervision, enforcement, guidance and outreach	Substantial
Mitigation measures applied by subject persons	
Risk understanding, assessment and management	Substantial
Customer due diligence related controls	Moderate
Reporting of STRs	Moderate
Resources dedicated to AML/CFT and staff knowledge (including MLROs)	High

9.4.4 Residual Risk

As indicated in the below table the overall residual risk of the sector is that of 'medium', and this is mainly driven by the risk of abuse through the disbursement of funds by VO (NPO) transactions including to high-risk jurisdictions. Here apart from encouraging financial access through the credit institutions, it is also important to have adequate programme planning and monitoring including local partners in high-risk jurisdictions.

Table 28: Residual risk ratings – VOs (NPOs)

Topic	**Threat**	**Effectiveness of mitigating measures**	**Residual risk**	**Overall residual risk level**
Disbursement of funds by VO (NPO) transactions including to high-risk jurisdictions	Medium-high	Moderate	Medium-high	**Overall risk rating = Medium**
Threat of TF abuse through raising of donations in Malta	Medium-high	High	Medium	
Threat of abuse of VOs (NPOs) for ML (including VOs related to sports)	Medium	Moderate	Medium	
Threat of ML related to misappropriation or mismanagement of VOs (NPOs) expenditures	Medium	High	Medium-low	
Administrators of VOs (NPOs) linked to ML/TF	Medium	High	Medium-low	
Funding of VOs (NPOs) for use of terrorist acts in Malta	Medium-low	High	Medium-low	

9.4.5 Recommendations

This section presents recommendations for subject persons to guide subject persons when applying preventative measures on a risk-based approach.

Update the TF risk understanding in the risk assessment and risk management strategies.

Have appropriate mechanisms to provide risk assessment information to competent authorities.

Align the policies, controls and procedures with the TF risk assessment
Measures should be commensurate with the level of risk, therefore, even where the risks are identified as lower in the TF risk assessment.

Monitor the implementation of the updated controls and enhance them, if necessary.

Continue monitoring TF sanctions updates, and news items relating to countries of concern.

Revisit the customer due diligence and enhanced customer due diligence, including transaction monitoring, in line with the findings of the NRA.

10 Sectoral Risk Assessments

This section presents findings of the sectoral risk assessments, by primarily sharing the findings of the financial services sector, followed by the DNFBPs, and the VFASPs.

Subject persons are to assess their risks not only based on the analysis in their respective sectoral section, but also on additional sections, such as, the overall ML risks 'section 11', 'section 12' that presents the TF risks, 'section 13' on PF and TFS related risks, as well as the other instruments as described in 'section 9'.

10.1 Financial services sector

This section presents the results of the risk assessments carried out on the financial sector that covers the banking sector, the financial institutions, the investments sector, the insurance sector, and the pensions sector.

10.1.1 Banking sector

By providing an extensive range of products and services to retail, corporate, institutional, and private banking customers, Maltese banks plays an important role in supporting the economic activity in Malta. Banks are also a key channel for international transactions into and out of Malta. In aggregate, as at end of 2022, the Maltese credit institutions were servicing some 1.4 million customers (2021: 1.3 million). In 2022 there were 20 credit institutions licensed under the Banking Act, with a further two (2) new licence applications that were being assessed by the MFSA. This implies that the number of credit institutions licensed under the Banking Act during the past four years has decreased (2019: 23, 2020:22, 2021:22, 2022:20).

10.1.1.1 ML threats in the banking sector

The ML threat analysis in the banking sector is mainly based on the analysis of the STRs, REQs and CBM data, and should be read in conjunction with section 11.1.1 "Money Laundering Threats". This section includes an analysis by predicate offences and ML typologies, where for example, the threat assessment included an analysis of the incoming international requests to Malta's law enforcement authority, where less than half of the international incoming requests received in 2021 involved banks in Malta due to these servicing customers which are the subject of the international incoming request.

Subject persons are to assess their risks not only based on the analysis in this sectoral section, but also on additional sections, such as 'section 12' that presents the TF risks, 'section 13' on PF and TFS related risks, as well as the other instruments as described in 'section 9'.

The large size of the customer base increases the sector's exposure to ML/TF and makes it more difficult to detect misuse of bank products for ML/TF purposes. While the customer portfolio is largely dominated by individual customers (97%), the banking sector still services a significant number of non-individual customers (circa 45,000). The sector's exposure to higher-risk customers

in absolute terms is primarily a result of its large customer base, but the exposure in proportion to the size of the customer base is low. Customers showing a higher threat category include customers operating in cash intensive businesses, PEPs, legal persons with an ownership structure that includes offshore vehicles, trusts and other legal arrangements including bearer shares and nominee shareholding, customers or beneficial owners benefitting from residence or citizenship by investment schemes, legal persons with foreign links and complex structures and customers transacting with VASPs, customers with connections to high-risk and non-reputable jurisdictions.

The substantial compliance costs incurred by banks, the pressure from correspondent banks and the increase in AML/CFT supervision and enforcement actions has led to credit institutions initiating de-risking exercises which resulted in the off-boarding of higher-risk customers. According to data collected by the FIAU for the calendar years 2020, 2021 and 2022, seven (7) banks terminated the business relationship with approximately 32,000 customers due to them being considered as posing a high ML/TF risk, or because such customers no longer satisfied a bank's customer acceptance policy. Such customers included customers benefitting from the Citizenship by Investment scheme, customers with no apparent substance in Malta, customers transacting with high-risk jurisdictions, customers having complex structures and customers to whom correspondent banking services were provided. Furthermore, during the four-year period ending 31 December 2022, in aggregate, a total of 8,000 customers were refused onboarding by banks due to such customers falling outside the risk appetite of banks. This implies that bank's risk appetite to service customers typically associated with higher risks has decreased, thereby resulting in lower risk exposure compared to previous years when de-risking initiatives were not commonly practiced.

Given that banks act as a medium for cash deposits, bank accounts can be used to place cash derived from proceeds of crime in the financial system. It was concluded that a significant number of STRs received in the three-year period ending 31 December 2020 which identified the use of cash have originated from credit institutions. Analysis of STRs submitted by credit institutions during the four-year period December 2021, indicated that the use of banking activities to facilitate suspected tax crimes approximately accounted for a major share of all STRs submitted. The involvement of natural persons featured in a number of STRs, with majority being domestic. However, the national tax risk assessment carried out in December 2021 concluded that the risk of abuse of Maltese bank accounts to launder proceeds of foreign tax is limited.

Although in the past years, the FIAU did not receive significant STRs from the banking sector that were flagged as possibly related to TBML the values associated with these cases were significantly higher than other cases involving other type of predicate offences.

During the years 2020 and 2021, the FIAU has received 39 and 25 STRs, respectively, with an indicator related to organised criminal groups (OCGs), thereby showing a reduction in this regard. This is the result of increased controls and monitoring by banks which makes it more difficult for OCGs to layer funds through the banking system.

Servicing non-resident customers and/or beneficial owners exposes banks to a heightened risk because funds used to process transactions through Maltese banks may be sourced from jurisdictions with poor AML/CFT control frameworks in place, leading to the risk of source of

funds being derived from illicit activities. However, during 2020, only approximately 1.5% and 10% of the customers and beneficial owners, respectively, were resident or incorporated in a non-EU/EEA jurisdiction, thereby limiting the ML/TF exposure from non-reputable and high-risk jurisdictions as listed in the FATF and EU list identifying high risk third countries with strategic deficiencies and jurisdictions featuring in the top 20 countries of the Basel Index.

Furthermore, since banks are considered as the core of Malta's financial system, they play a key role in facilitating financial flows into and out of the country. This exposes banks to foreign jurisdiction risk due to the risk of banks serving as a channel to facilitate international movement of proceeds of crime or for TF. The risk exposure increases if transactions originate from or are remitted to non-reputable jurisdictions and high-risk jurisdictions. Data collected by the CBM indicates that 71% of the total value of cross-border payments were remitted to and/or received from EU countries, whereas 29% were linked to non-EU countries, with United States of America, Switzerland and South Africa featuring as the three (3) top countries.

Table 29: ML threats - banking sector

Threat	Impact	Likelihood	Threat level
Exposure to high-risk jurisdictions due to the processing of international payments	Significant	Very Likely	High
Exposure to jurisdictions as a result of servicing non-resident customers and/or BOs	Significant	Likely	Medium-high
Use of bank accounts to place cash derived from proceeds of domestic crime in the financial system	Significant	Likely	Medium-high
Use of bank accounts to launder proceeds of domestic tax crime	Moderate	Very Likely	Medium-high
Trade-based ML	Significant	Possible	Medium-high
Abuse of bank accounts by higher-risk customers (e.g., PEPs, customers benefitting from CBI/RBI schemes, cash intensive business, legal persons with an ownership structure that includes offshore vehicles, trusts and other legal arrangements and legal persons with foreign links and complex structures and customers transacting with VASPs	Significant	Possible	Medium-high
Use of bank accounts to launder proceeds of foreign tax crime	Significant	Unlikely	Medium
Criminals and their associates being the beneficial owner of, holding a significant or controlling interest or holding a management function in a credit institution	Severe	Very unlikely	Medium
Use of bank account by OCGs	Significant	Unlikely	Medium
Use of bank accounts to launder of bribery and corruption	Moderate	Possible	Medium

10.1.1.2 Vulnerabilities

It was established that credit institutions are subject to an overall 'medium' level of inherent vulnerability related to ML. This assessment falls into two broad categories, namely, delivery channels and products/services.

Face-to-face customer contact across all sectors has declined, and the banking sector is no exception to this. In fact, data collected shows that in 2022, 50% of customers were on-boarded through a non-face-to-face method. Furthermore, many customers are now making larger use of remote service delivery channels such as ATMs and online/mobile/phone banking. Such digital facilities expose the banking sector to increased ML/TF vulnerabilities due to the non-face-to-face interaction. In particular, customers applying for banking products remotely may not be subject to visual identification making it easier for perpetrators to impersonate a customer to transact anonymously and to distance themselves from illicit activities. ATMs may be exploited by criminals to launder money by depositing illicit cash into the financial system as well as to facilitate funding of terrorism through cash withdrawals. Unlike over-the-counter deposit, ATMs allow cash to be deposited without contact with bank representatives (although deposit thresholds are in place).

According to data for the years 2019 and 2020, credit institutions appear to be growing averse to on-boarding customers through introducers. In fact, whereas in 2019, 43% of banks accepted the on-boarding of customers via introducers, the 2020 figure dropped to 30%. Furthermore, all banks remarked that due diligence is carried out on introducers. Customers onboarded through introducers without direct contact with bank representatives increases the ML/TF vulnerability to credit institutions, especially if the AML/CFT internal controls and procedures of the introducers are not robust.

Credit institutions offer an array of products to customers, including transaction accounts, pooled accounts, correspondent banking, trade finance, safe deposit boxes, prepaid cards, merchant acquiring, cheques and loans. Each product has a different level of inherent ML/TF vulnerability. Transaction accounts are the most used within the banking sector, with approximately 773,600 customers having access to a transaction account. 94% of such customers are individual customers, whereas 6% are non-individual customers. According to STR data received by the FIAU during the year 2021, transaction accounts are the most misused product, in the range of 45% to 50%. These accounts enable fast movements of funds both domestically and internationally, and are also used as a transit point for cash deposits and withdrawals. The large number of transactions processed daily through these accounts also heightens the ML/TF vulnerability. Other initiatives, such as SEPA-Instant Payments Scheme[61] and ACH Network[62] are increasingly speeding up payments into real-time payments. This creates difficulties for banks to monitor transactions, particularly in monitoring real-time transactions. Additionally, in accordance with REQ data for 2021, there appears to be some 4,190 pooled accounts, with the total value of transactions flowing through pooled accounts during 2020 amounting to circa €20BN. Although these pooled accounts are opened and administered by customers who in most cases are also subject to AML/CFT obligations, such accounts still carry an ML/TF vulnerability if the account is misused, such as

[61] https://www.europeanpaymentscouncil.eu/what-we-do/sepa-instant-credit-transfer
[62] https://www.nacha.org/

processing operational transactions on behalf of customers or if weak controls are applied by customers in the operation of such accounts.

While safe deposit boxes are vulnerable to ML/TF due to customers' ability to place assets in such facilities without the scrutiny of bank representatives, the degree of vulnerability is reduced due to the low number of customers being provided with such service in comparison with the total number of customers. It was also noted that the provision of safe deposit boxes offering by banks is on a decline. Moreover, the two major players have exited the market in recent years and have only been servicing existing clients of such products or legacy clients.

Similarly, while the pre-paid card market has increased in its popularity globally, the Maltese banking sector has registered a decrease in this regard. Although the use of cheques in Malta is still significant, the introduction of the CBM of Directive 19 on the use of cheques and bank drafts, which came into force as from January 2022, limited the transferability of cheques and thus acted as an effective mitigating measure for the main vulnerability of such product. This has reduced their exploitation by money launderers to conceal the audit trail of illegal funds flowing in the financial system.

Table 30: Rating of the vulnerabilities - banking sector

Vulnerability	Impact	Exposure	Vulnerability level
Transactional accounts	Significant	Very high	High
Pooled accounts	Moderate	Very high	Medium-high
Trade finance	Significant	Moderate	Medium -high
Non-face-to-face onboarding	Moderate	Moderate	Medium
Online banking	Moderate	High	Medium
ATMs	Moderate	High	Medium
Correspondent banking	Severe	Low	Medium
Cheques	Moderate	High	Medium
Loans	Minor	High	Medium-low
Introducers	Moderate	Low	Medium-low
Safe deposit boxes	Moderate	Moderately low	Medium-low
Prepaid cards	Moderate	Moderately low	Medium-low
Merchant acquiring	Moderate	Moderately low	Medium-low
Face-to-face onboarding	Negligible	Moderate	Low

10.1.1.3 Effectiveness of mitigating measures

The serious breaches of AML obligations that took place in two (2) credit institutions which were identified during compliance examinations undertaken in 2018 have served as crucial lessons to Malta to accentuate the importance of AML. Both cases have received a lot of public attention, both locally and internationally, and demonstrated the authorities' commitment and strength in detecting and enforcing effective and proportionate measures for serious breaches of AML obligations. The MFSA has also taken effective measures for the risks identified in both credit institutions, leading to the ECB withdrawing the banking licence of both institutions based on MFSA's proposal.

These cases have also contributed to governmental commitment to increase budgets and resources allocated to authorities responsible for the banking sector licencing, supervision and enforcement, thereby leading to enhanced processes in these areas. However, the effectiveness of the process implemented by the FIAU is being greatly undermined by delays in judicial proceedings. Indeed, a number of appeals filed against administrative sanctions issued by the FIAU have been pending for more than the six (6) months set out by law. In addition to this, appeals to sanctions imposed by the FIAU are heard by the Court of Appeal (Inferior Jurisdiction), and being a general Court, the level of expertise necessary to confirm or otherwise the breaches determined by the FIAU and what factors to consider as to whether a sanction is proportionate, dissuasive and effective may be weak. Furthermore, upon appeal, most administrative penalties imposed by the FIAU are substantially reduced by the Court. The Court's reasoning for reducing the quantum to such levels is not explained nor is any explanation provided as to how the now reduced penalty can still be considered as being proportionate, effective and dissuasive. This happens even when the same court would have confirmed all, or the greater part of the breaches as identified by the FIAU, as well as their materiality and severity. Notwithstanding the above, except for few banks, sanctions imposed by the FIAU on credit institutions are not appealed, with the latter also agreeing to implement the directives imposed by the FIAU to address any gaps identified in their AML/CFT framework.

The FIAU has also increased its outreach and training efforts with the objective of improving the banks' knowledge of their AML/CFT obligations and instilling an enhanced compliance culture across this sector. In 2021, the FIAU has also introduced AML Clinics specifically for the Banking Sector with the aim of creating a forum for discussion between banks allowing for the sharing of expertise and best practices across the sector. Other external factors introduced in recent years such as the Central Bank Account Register (CBAR) and the CBM's MTEUROPAY payment system also play important mitigating measures on the banking sector.

Furthermore, the banking sector has also improved its understanding of ML risks and the design of AML control frameworks, often through substantial investments in solutions and resources to assist in the implementation of AML compliance programs. This has in turn led to an increase in suspicious transactions reporting to the FIAU. Notwithstanding this, the carrying out of customer risk assessments for the purpose of understanding the risk exposure stemming from servicing specific customers is an area deemed to require improvement by banks to guide towards the better application of the risk-based approach in relation to the CDD measures to be applied with respect to their customer portfolio. Monitoring of customer relationships and scrutiny of transactions is also at the forefront of an effective AML framework and these measures also need further improvement by banks. A better risk understanding and monitoring, including better application of the risk-based approach would also lead to improvement in the quality of STRs submitted by banks.

Table 31: Effectiveness of mitigating measures - banking sector

Mitigating measures applied at national level	
Controls applied by Supervisory Authorities in relation to licencing, supervision, enforcement, guidance and outreach	High
Other external factors impacting the AML/CFT framework in place (e.g. CBAR and participation in payment systems)	High
Mitigation measures applied by banks	
Risk understanding, assessment and management	Moderate
Customer due diligence related controls	Substantial
Reporting of STRs	Substantial
Resources dedicated to AML/CFT and staff knowledge (including MLROs)	High

10.1.1.4 Residual risk analysis

As indicated in table 32 the overall residual risk of the banking sector is 'medium'.

Table 32: Residual ML risk analysis - banking sector

Topic	Inherent risk	Effectiveness of mitigating measures	Residual risk	Overall residual risk level
Trade-based ML	Medium-high[63]	Moderate	Medium-high	**Overall residual risk level = Medium**
Use of bank accounts to launder proceeds of domestic tax crime	Medium-high	Substantial	Medium - high	
Exposure to high-risk jurisdictions due to the processing of international payments	Medium-high	Substantial	Medium-high	
Use of bank accounts to place cash derived from proceeds of crime in the financial system	Medium-high	Substantial	Medium-high	
Use of bank accounts to launder proceeds of foreign tax crime	Medium	Substantial	Medium	
Use of bank account by OCGs	Medium	Substantial	Medium	
Use of bank accounts to launder proceeds of bribery and corruption	Medium	Substantial	Medium	
Abuse of system via customers transacting with VFAPSPs	Medium-high	High	Medium	
Exposure to jurisdictions as a result of servicing non-resident customers and/or BOs	Medium-high	High	Medium	
Criminals and their associates being the beneficial owner of, holding a significant or controlling interest or holding a management function in a credit institution	Medium	High	Medium-low	
Abuse of bank accounts by PEPs	Medium	High	Medium-low	
Abuse of system via customers benefitting from CBI/RBI schemes	Medium	High	Medium-low	

The table above indicates that domestic tax crime and trade-based money laundering, have a 'medium-high' residual risk rating. The risk of domestic tax crime stems both from natural and corporate customers. Corporate customers may use bank accounts to facilitate trade-based money laundering, whereby customers use trade transaction to legitimise the illicit origin of funds. Furthermore, modern technology is making it easier to forge documents and this can be exploited by banking customers to create false documents that support transactions processed. Therefore, unless the banking sector has robust detection mechanisms in place, transactions which have indications of trade-based money laundering may go undetected. Banks are also mostly exposed

[63] This rating is based significantly on an inherent threat of this international phenomena, rather than on specific TBML indicators found in Malta.

from transaction accounts, which process a lot of transactions, therefore the implementation of effective risk-based transaction monitoring measures will enable banks to monitor transactions taking place and generate alerts that require further scrutiny. Through the effective implementation of such measures, it will lead to more effective reporting to the FIAU.

10.1.1.5 Recommendations

This section presents sector specific recommendations to guide subject persons when applying preventative measures on a risk-based approach.

Enhancing the risk-based approach

- Banks should align the business risk assessment and the customer risk assessment with the results of the NRA and take steps to update the customer risk profiles as part of ongoing monitoring procedures, thereby ascertaining the risks identified are current.
- Banks should also review their CDD procedures, both at onboarding stage and as part of their ongoing monitoring obligations, to ascertain that these are risk-based, reflect the outcome of the NRA and are commensurate with the risks identified.

Monitor the effectiveness of transaction monitoring systems for national and emerging risks

Banks should assess the effectiveness of their transaction monitoring systems to ascertain that these allow proper detection of transactions that may be related to national or emerging risks, such as cash transactions relating to criminal proceeds, misuse of pooled accounts, and transactions with TF, trade-based money laundering or tax crime indicators. Banks should also ensure that assessment of the effectiveness of their transaction monitoring system also takes into consideration the submission of good quality and material STRs.

Continue taking remedial action to address weaknesses in the AML/CFT control framework

Banks should continue to take steps to assess the effectiveness of their AML/CFT control frameworks (e.g., through internal audits) and take action to address any weaknesses identified, such as through the implementation of self-imposed remedial action plans and through cooperation with supervisory authorities to address any shortcomings identified during supervisory examinations.

10.1.2 Financial institutions

As at December 2022, 50 financial institutions were authorised to carry out business under the Financial Institutions Act (Chapter 376). These financial institutions fall under fall in two broad categories:

1) Institutions undertaking payment services and/or the issuance of electronic money (40)
2) Institutions undertaking lending activities (8) and money brokering activities (2)

This sector has experienced a sizeable growth both in terms of number of licence holders and business volume, mainly in so far as payment services institutions and electronic money institutions are concerned, where a total of ten (10) financial institutions were licenced during the three-year period ending 31 December 2022. The growth in the payments industry is mirrored at a European level with client behaviour favouring digital payments over traditional means. This has accelerated over 2021 during the COVID-19 pandemic with consumers utilising less cash to conduct payments. Changes in the payments landscape, including the emergence of instant payments, in addition to constant advancement in new technologies are further trends facilitating the growth of digital payments. During the same period, there were 12 surrendered/cancelled licences as a direct consequence to the sustained supervisory presence leading to significant supervisory and regulatory action.

Subject persons are to assess their risks not only based on the analysis in their respective sectoral section, but also on additional sections, such as, the overall ML risks 'section 11', 'section 12' that presents the TF risks, 'section 13' on PF and TFS related risks, as well as the other instruments as described in 'section 9'.

10.1.2.1 ML/TF/PF/TFS threats

Data from the FIAU REQs indicates that, as at end of 2022, the FI sector serviced approximately 3.7 million customers in comparison to 1.4 million customers by the Maltese banks (a significant increase when compared to 2020). Similar to the banking sector, the FI sector is largely dominated by individual customers (79%), however there is still a significant number of non-individual customers (21%), which nowadays increasingly have complex structures. FIs also offer services to unbanked customers (both retail and commercial clients) or customers which have been de-risked by credit institutions.

A number of FIs also offer services to higher-risk business sectors including virtual financial assets (VFAs) by collecting fiat payments or issuing e-money to be subsequently exchanged for VFAs by the exchanges. In fact, payment volumes to VFASPs have increased significantly over the past few years, and the trend suggests that there will continue to be significant growth in this area. The link between the FI sector and the VFASP sector is also highlighted through two (2) newly licenced FIs who operate in the same group of companies as two (2) licenced VFASPs.

In accordance with data collected by the CBM, during the year 2021, FIs executed circa €21bn payment transactions, representing a 76% increase over the previous year (€12bn). This was mainly driven by the provision of 'correspondent banking' services by one licence holder, the significant growth by other FIs, and the migration of UK business to a number of new licence

holders following Brexit. Whereas a large proportion of the financial flows are within Malta, when it comes to cross-border transactions in 2021, the total transfers to EU/EEA countries amounted to 75.9% whereas the total transfers to non-EU/EEA countries amounted to around 24%. E-money transactions and credit transfers amounted to 90% of transactions with EU/EEA countries, whereas money remittance and credit transfers accounted for 90% of transaction with non-EU/EEA countries. Furthermore, payment statistics as at December 2021 collected by the CBM indicate that around 60% of money remittance payments were sent to third countries, mainly as a result of the third country nationals working in Malta and remitting their funds to their countries.

This flow of funds from Malta has also been considered from the TF point of view in the TF working paper. Additionally, since FIs act as a medium to facilitate significant international payments to/from Malta, this exposes FIs to foreign jurisdiction risk since funds used to process transactions may be sourced from jurisdictions with poor AML/CFT control framework in place, leading to the risk of source of funds being derived from illicit activities or that funds relate to TF.

Analysis of STRs received by the FIAU from this sector indicated that the top suspected predicate offence is fraud followed by tax-related crimes. In a sector which is defined by non-face-to-face business, threats from fraudulent activities such as investment scams, document forgery, identity theft and debit/credit card fraud are more likely to materialise. As explained in the introduction to this section, data available to the FIAU also indicates an increase in servicing corporate customers which are part of complex structures, thereby also increasing the potential threat of foreign tax crime, a threat that was analysed in detail in the legal persons working paper.

With regards to international requests for information received by the FIAU in 2021, there were a moderate number that involved clients of FIs in their request. It was noted that there was the involvement of only one (1) FI in the ML investigations by the MPF in 2021.

In line with the analysis carried out on FIs, the rating of the threats is as follows.

Table 33: Rating of the ML/TF/PF/TFS threats – FIs

Threat	Impact	Likelihood	Threat level
Jurisdictional risk exposure due to international payments	Severe	Likely	High
Exposure to high-risk jurisdictions due to non-resident customers and/or BOs	Significant	Very likely	High
Misuse of FIs services from higher-risk customers (including underbanked customers)	Significant	Likely	Medium-high
Misuse of FI sector for fraudulent activities	Significant	Likely	Medium-high
Abuse of the sector to launder proceeds of foreign crime including tax crime	Significant	Possible	Medium-high
Misuse of FI services by customers who are part of complex corporate structures	Significant	Possible	Medium-high
Abuse of the sector by customer transacting with VFA exchanges	Significant	Possible	Medium-high
Abuse of the sector to launder proceeds of domestic crime including tax crime	Moderate	Likely	Medium
Criminals and their associates holding or being the beneficial owner of a significant or controlling interest or holding a management function	Severe	Very unlikely	Medium

10.1.2.2 Vulnerabilities

FIs operate varied business models, mostly via non-traditional delivery channels, leveraging on technology to onboard and service customers remotely, thereby increasing the interface risk. The use of agents by FIs to service customers also increases the risks associated with this sector. Agents are not subject persons themselves and, though they should be subject to review by the FI that has appointed them, they may still implement weak AML/CFT controls on which FIs would be reliant, particularly if the agents' core business is not linked to the financial services industry.

Risks are also heightened due to the volume and speed of transactions since transactions potentially linked to ML/TF may be identified after the payment is processed. The payments industry is experiencing an exponential growth as witnessed during the COVID-19 pandemic where contactless payments and additional access to financial services came to the fore. Other initiatives, such as SEPA-Instant Payments Scheme[64] and ACH Network[65] are increasingly speeding up payments into real-time payments. These developments can render the application of AML/CFT obligations more difficult, but the response so far has been slow, thereby leading to potential gaps in regulation. Therefore, this is not only Malta specific but a horizontal vulnerability at an international level that needs to be addressed.

[64] https://www.europeanpaymentscouncil.eu/what-we-do/sepa-instant-credit-transfer
[65] https://www.nacha.org/

Furthermore, particularly in relation to money remittance services, this sector is also vulnerable to one-off type transaction without the opening of a payment account. In such cases, since the FI does not enter into a business relationship with the customers, CDD obligations may be less stringent, with some occasional transactions also being exempt from the application of CDD measures due to their low value.

The use of virtual IBANs by payment institutions has also been assessed as an emerging risk, particularly since the fact that various virtual IBANs are linked to one IBAN account may lead to weaknesses in customer profiling and transaction monitoring, and these are not currently reportable on CBAR.

The ratings of the vulnerabilities in this sector are as follow:

Table 34: Rating of the vulnerabilities - FIs

Vulnerability	Impact	Likelihood	Vulnerability level
Conducting CDD and having all relevant documentation in the absence or a limited local footprint	Severe	High	High
Developments such as virtual IBAN	Significant	Moderate	Medium-high
Abuse of the shareholding structure and the BO involvement	Significant	High	Medium-high
Volume and speed of payments	Significant	High	Medium-high
Interface risk: non-face-to-face customer onboarding and service	Moderate	High	Medium
Interface risk: Use of agents/intermediaries	Moderate	High	Medium

10.1.2.3 Effectiveness of mitigating measures

In assessing the effectiveness of mitigating measures in place the analysis took into consideration:

- Controls put in place by regulators, namely the FIAU and MFSA, through the supervision carried out on FIs both in terms of checks at licencing and authorisation stage to prevent the entry of bad actors in the sector as well as through ongoing monitoring to ensure that FIs are operating in line with the applicable legislative provisions, and
- AML/CFT compliance programmes set up by FIs to prevent being used by their customers as a vehicle to facilitate ML/TF.

With regards to the national controls, in the past years, the MFSA has enhanced its licensing process through the implementation of a robust structured and risk-based process to ensure that only applicants that demonstrate compliance with the regulatory framework are authorised. The MFSA has set and published an authorisation risk appetite statement as well as guidelines on the fitness and properness process aimed at ensuring that suitable individuals occupy key positions in licensed FIs. As a result of the stricter standards introduced by the MFSA, as part of the authorization process, the MFSA has terminated the licensing process of six (6) applicants in 2021 (2 in 2020) and has set more intrusive pre-commencement and post-commencement conditions on new license holders. Higher level of scrutiny is applied via the Fitness and Properness assessments

whereby a framework has been implemented requiring the Authority to hold interviews with applicants who would be holding key function in high-risk/high impact FIs.

The FIAU and the MFSA (acting as agents of the FIAU) also carried out several compliance reviews on a number of FIs, with the aim of monitoring adherence to AML/CFT regulatory obligations. Apart from the increase in the AML/CFT supervisory coverage, the period 2019 to 2021 has also experienced an increase in the number of dissuasive enforcement measures being applied by the FIAU on FIs that fail to adhere to AML/CFT obligations. However, the effectiveness of the process implemented by the FIAU is being greatly undermined by delays in judicial proceedings. Indeed, a number of appeals filed against administrative sanctions issued by the FIAU have been pending for more than the six (6) months set out by law. In addition to this, appeals to sanctions imposed by the FIAU are heard by the Court of Appeal (Inferior Jurisdiction), and being a general Court, the level of expertise necessary to confirm or otherwise the breaches determined by the FIAU and what factors to consider as to whether a sanction is proportionate, dissuasive and effective may be weak. Furthermore, upon appeal, most administrative penalties imposed by the FIAU are substantially reduced by the Court. The Court's reasoning for reducing the quantum to such levels is not explained nor is any explanation provided as to how the now reduced penalty can still be considered as being proportionate, effective and dissuasive. This happens even when the same court would have confirmed all, or the greater part of the breaches as identified by the FIAU, as well as their materiality and severity.

Furthermore, when assessing the external factors, it is to be noted that FIs participating in the CBM's MTEUROPAY payment system are also expected to implement robust AML/CFT control frameworks. Participants undergo a thorough due diligence assessment process as part of the authorisation process applied by CBM for the purpose of joining the MTEUROPAY.

With regards to the sectoral controls, however it is to be noted that the compliance structure within the FI sector still presents a number of weaknesses as evidenced by the compliance failures identified as part of AML/CFT supervision carried out by the FIAU, including six (6) fines in 2021 exceeding a total of €2 million. Common deficiencies in AML/CFT related controls included poor application of risk management procedures, weaknesses with customer identification and verification processes, gaps in transaction monitoring procedures failure to collect proper source of wealth/funds information and weakness in record keeping procedures. Despite the volume and speed of transactions processed by FIs, 17% of FIs relied on manual transaction monitoring during 2021 (still presenting an improvement when compared to 2020 when reliance on manual transaction processes stood at 20%). Furthermore, significant weaknesses were identified in the transaction monitoring systems in 11 out of 18 compliance examinations carried by the FIAU in 2020 and 2021. It is also to be noted that the FI sector has registered an increase of 94% of STRs submitted between 2020 and 2021. The STRs submitted by this sector account for 7% of the total STRs submitted by subject persons to the FIAU in 2021.

Typically, FIs operate with a leaner internal governance structure compared to credit institutions, which in turn increased risks emanating from weak governance structures, with issues presenting themselves within board and management structures, internal controls and resulting in key person dependency risk and a poor compliance culture. This risk is higher in instances where a significant degree of shareholder intervention is experienced, thereby possibly undermining the independence

of the board and management. In fact, MFSA data indicates that shareholding structures in 19 FIs include a single individual holding 75% or more of the issued share capital. A further assessment of the roles played by the beneficial owners within the institutions, indicates that 53% occupy multiple roles, sitting on the Board of Directors and holding an executive managerial role. A further 21% sit on the Board of Directors only, while another 21% have no direct role in the institution. The FI sector also has a higher rate of turnover in key function holders (i.e., Board of Directors, executive management, and heads of internal control functions). This is driven by the shortage of adequately skilled individuals in the local market.

Given the above, on average, the overall level of effectiveness of mitigating measures is evaluated to be 'substantial'. On a national level, improvements are required with regards to the level of dissuasiveness of enforcement measures following appeals by FIs for sanctions imposed by the FIAU as a result of breaches of AML/CFT obligations. Moderate improvements are needed with regards to prudential supervision, AML/CFT guidance and outreach, and other external factors impacting the AML/CFT framework in place (pressures from correspondent banks, participation in payment systems). Moderate improvements are needed on the level of AML/CFT supervision, and the licensing and authorisation process, with major improvements required on the guidance and outreach. On a sectoral level, major improvements are required on the application of risk assessment procedures, transaction (including cash) monitoring and customer profiling, the MLRO turnover rate, the customer due diligence related controls, and the overall resources and the internal governance. This will in turn lead to an improvement in both quantity and quality of the suspicious reports sent to the FIAU.

The results of the assessment are as follows:

Table 35: Effectiveness of mitigating measures - FIs

Mitigating measures applied at national level	
Controls applied by supervisory authorities in relation to licencing, supervision, enforcement, guidance and outreach	Substantial
Other external factors impacting the AML/CFT framework in place (e.g., pressures from correspondent banks, participation in payment systems)	Substantial
Mitigation measures applied by FIs	
Risk understanding, assessment and management	Substantial
Customer due diligence related controls	Moderate
Reporting of STRs	Substantial
Resources dedicated to AML/CFT and staff knowledge (including MLROs)	Moderate
Internal governance	Moderate

10.1.2.4 Residual risk analysis

The overall residual risk rating of the FI sector is found to be 'medium-high'. The highest rating is in relation to the exposure to high-risk jurisdictions due to international payments and non-resident customers/beneficial owners, the risk in relation to the exposure to higher-risk customers, using FIs to launder the proceeds of foreign tax crime and the laundering of money by complex corporate structures.

Table 36: Residual Risk Ratings - FIs

Topic	Inherent Risk	Effectiveness of mitigating measures	Residual risk	Overall residual risk level
Jurisdictional risk exposure due to international payments	High	Moderate	High	**Overall residual risk rating = Medium-high**
Misuse of FIs services from higher-risk customers (including underbanked customers)	High	Substantial	Medium-high	
Exposure to high-risk jurisdictions due to non-resident customers and/or BOs	Medium-high	Moderate	Medium-high	
Use of FIs to launder proceeds of foreign tax crime	Medium-high	Moderate	Medium-high	
Misuse of FI services by customers who are part of complex corporate structures	Medium-high	Moderate	Medium-high	
Misuse of FI sector for fraudulent activities	Medium-high	Moderate	Medium-high	
Abuse of the sector by customer transacting with crypto exchanges	Medium-high	Moderate	Medium-high	
Use of FIs to launder proceeds of domestic tax crime	Medium	Moderate	Medium	
Criminals and their associates holding or being the beneficial owner of a significant or controlling interest or holding a management function	Medium	High	Medium-low	

10.1.2.5 Recommendations

This section presents a number of recommendations to guide subject persons when applying preventative measures on a risk-based approach.

Enhancing the risk-based approach

- FIs should review their business risk assessment and the customer risk assessment to align it with the results of the NRA and ensure that they update the customer risk profiles, when necessary, as part of ongoing monitoring procedures, thereby ascertaining the risks identified are current.
- FIs should also review their CDD procedures, both at onboarding stage and as part of their ongoing monitoring obligations, to further ascertain that these are risk-based, reflect the outcome of the NRA and are commensurate with the risks identified.

Monitor the effectiveness of transaction monitoring systems for national and emerging risks

FIs should assess and monitor the effectiveness of their transaction monitoring system to ascertain that these allow proper detection of transactions that may be related to national or emerging risks, transactions connected to high-risk jurisdictions, transactions with crypto exchanges and transactions with TF, fraud and tax crime indicators. FIs should also ensure that assessment of the

effectiveness of their transaction monitoring system also takes into consideration the submission of good quality and material STRs.

Take remedial action to address weaknesses in the AML/CFT control framework
FIs should take steps to assess the effectiveness of their AML/CFT control frameworks (e.g., through internal audits) and take action to address any weaknesses identified, such as through the implementation of self-imposed remedial action plans and through cooperation with supervisory authorities to address any shortcomings identified during supervisory examinations.

Improving internal governance
The Management Body plays a crucial role in the implementation of an effective AML/CFT control framework within financial institutions. It is therefore imperative that, amongst others, the Management Body (i) provides the MLRO and its monitoring function with sufficient resources, including appropriate staff and technological means, to ensure that they can carry out their obligations effectively, (ii) provides the MLRO with full and unlimited access to records, data and documentation for the purpose of fulfilling his/her responsibilities, (iii) requests regular oversight reporting, including non-compliance reporting and (iv) ensures that employees are knowledgeable of the provisions of the PMLFTR and the measures, policies, controls and procedures applied in this regard.

10.1.3 Investment services sector

This section presents the results of the assessment carried out on the risk of laundering of proceeds of crime and the funding of terrorism in the investment services sector. The said sector is regulated by the MFSA while the FIAU oversees AML/CFT regulation. The investments sector includes Investment Firms, Fund Managers (Alternative Investment Fund Managers (AIFMs), Undertakings for Collective Investments in Transferable Securities (UCITS) Management Companies and De-Minimis Fund Managers), Collective Investment Schemes (Alternative Investor Funds (AIFs), UCITS Funds and Professional Investor Funds (PIFs))(collectively referred to as CISs), Recognised Persons (Recognised Fund Administrators, Recognised Incorporated Cell Companies and Private Schemes) and Depositaries of Collective Investment Schemes.

Data sourced from the MFSA indicates that this sector is the largest within the wider financial services sector. As at the end of 2021, the sector included 148 Investment Service Providers, 222 CISs, 503 sub-funds of CIS, and 38 Notified AIFs. Assets under management amount to €30.19 (231% of GDP[66]) billion for Maltese Asset Managers, whilst the net asset value for Malta-domiciled funds stood at €20.41 billion (with only €4 billion relating to Maltese residents) as at end 2021.

Subject persons are to assess their risks not only based on the analysis in their respective sectoral section, but also on additional sections, such as, the overall ML risks 'section 11', 'section 12' that presents the TF risks, 'section 13' on PF and TFS related risks, as well as the other instruments as described in 'section 9'.

10.1.3.1 ML/TF/PF/TFS threats

Data sourced from FIAU REQs submitted by CISs suggest that over 96% of funding is being done through the banking system, with the remaining 3% being done through subscriptions in kind and 0.08% through internet-based, mobile applications or other e-money/e-wallet services. Similarly, 67.4% of investment firm funding is done through the banking system and 29.8% through internet-based, mobile applications or other e-money/e-wallet services (to note that transfers from banks or other licenced entities would be required to fund such applications/wallets). It is to note that a very small number of investment firms and CISs have reported a minimal use of cash, at 0.07% and 0.06%, respectively.

On the basis of data collected from competent authorities such as the FIAU and the MTCA, there are indications that the investment sector may be targeted to launder the proceeds of tax crimes, corruption and bribery, fraud, forgery, and organised crime. While the number of reports and requests received was not in itself considerable, one has to take in account the fact that this sector is characterised by a high number of non-resident customers. Indeed, Maltese investors in collective investment schemes in 2021 only totalled 14%, with the remaining being foreign resident/established admittedly the greater part in reputable jurisdictions. The same applies with regards to the location where collective investment schemes invest. Thus, the sector is characterised by a significant non-resident customer base.

[66] The GDP data is in line with the news release no. 037/2022.

Data for 2021 indicates that there are very few reports submitted by subject persons that involved investment services licensees. Meanwhile, from the STRs submitted by the investment services, the top predicate offences were in relation to tax crimes, corruption and bribery, fraud, forgery, and organised crime.

Furthermore, it is to be noted that the MTCA received only four (4) international administrative requests between the period 2019-2021, in relation to private equity and investment with the amount involved being significant. Furthermore, there was another request that was dealt with criminally and where the asset involved was in relation to private equity and investment, and the amount involved in monetary terms was again relatively high.

Criminal investigations that involved the use of an investment service provider in 2020 were six (6), and investigations that involved investment services agencies in 2021 there were another six (6). In 2021 the Asset Recovery Bureau had as frozen investment assets a total of €2.4 million. These assets included company shares, investment portfolios and shares held in investment funds.

Given these key findings, the ratings for the threats prior to assessing the controls, are:

Table 37: Rating of the ML/TF/PF/TFS threats – investment services sector

	Impact	Likelihood	Threat level
Sector specific threats			
Misappropriation of funds	Significant	Possible	Medium-high
ML arising from organised crime	Significant	Possible	Medium-high
Launderings proceeds of foreign tax crime	Significant	Likely	Medium-high
Criminals and their associates holding or being the beneficial owner of a significant or controlling interest or holding a management function.	Severe	Very unlikely	Medium
Laundering of proceeds of foreign bribery and corruption	Significant	Unlikely	Medium
Abuse of legal persons and arrangements for laundering of proceeds from domestic tax crime	Moderate	Possible	Medium
Collective investment schemes			
Exposure to high-risk jurisdictions	Significant	Possible	Medium-high
Investment firms			
Exposure to high-risk jurisdictions	Significant	Unlikely	Medium
Recognised fund administrators			
Exposure to high-risk jurisdictions	Significant	Unlikely	Medium

10.1.3.2 Vulnerabilities

The vulnerabilities analysed were in relation to the AML/CFT framework and the governance of the subject persons. One of the main vulnerabilities in this sector is due to the widespread use of nominees and similar arrangements to hold investments. This can be especially seen in the context of collective investment schemes which can cause major difficulties in determining who is actually the underlying investor as nominees, primarily foreign ones, and may either be reticent or may not themselves know due to a chain of nominee holdings.

There is another vulnerability in relation to crowdfunding where to date European Crowdfunding Service Providers (ECSPs) are not deemed to be subject persons in terms of the PMLFTR or subject persons in terms of Directive (EU) 2015/849.

Furthermore, some services in the investment services area may be offered through online means such as online brokerage services where non-face-to-face business is undertaken. This poses an additional AML/CFT vulnerability due to the lack of transparency and challenges in carrying out CDD/KYC, increased trading volumes and high frequency/algorithmic trading, and heightened risk of cyber or intruder attacks.

In terms of investments made, collective investment schemes and investment services providers may sometimes invest in emerging new assets with a higher degree of risk, where in 2021, the exposure stood at 2%. They may also carry out their investments' activity through Special Purpose Vehicles (SPVs) and multiple jurisdictional layers which may be synonymous with lack of transparency and non-cooperative.

In view of these key findings, the rating of vulnerabilities is as follows:

Table 38: Rating of vulnerabilities – investment services sector

Vulnerability	Impact	Likelihood	Vulnerability level
Determining the underlying investor in nominee relations	Significant	Moderately low	Medium
Product related vulnerabilities			
Delivery channels – Face-to-face onboarding	Negligible	Moderate	Low
Investments in new emerging assets vulnerable to financial crime	Moderate	Moderately low	Medium-low
Delivery channels – non-face-to-face onboarding	Moderate	Moderate	Medium
Crowdfunding platforms that are not included as subject persons	Moderate	Moderate	Medium

10.1.3.3 Effectiveness of mitigating measures

At licensing stage, competency assessments and due diligence checks are performed throughout the MFSA pre-authorisation process. Applicants with ties to high-risk jurisdictions are either not authorised or subject to enhanced monitoring and ongoing due diligence assessments, depending on the application being considered. Complex structures are vetted, and checks are conducted on the beneficial owners as well as the source of the invested capital. In this regard, the MFSA questions capital inflows into Investment Services Providers in relation to SoW/SoF. The Due Diligence Function within the MFSA also screens for sanctions, PEPs and adverse media on a daily basis, searching for links to regulated entities and related third parties.

The supervisory activities performed by the relevant authorities have resulted in a number of enforcement and administrative measures. Particularly, in 2020 and 2021, five (5) companies were fined a total of €1.6 million by the FIAU for compliance failures detected during supervisory

examinations. Other administrative penalties imposed in 2020 and 2021 were on 12 companies which either failed to submit or submitted late the annual risk evaluation questionnaires, and 20 companies for either failing to reply or replied late to requests for information made by the FIAU. 32 remediation actions and plans were required in addition to seven (7) closure letters. Guidance on specific areas such as the Business Risk Assessment are published by the FIAU to the industry. The issuance of sector specific Implementing Procedures is also in the pipeline. Through the above, both the FIAU and the MFSA have worked towards raising the bar when it comes to AML related requirements and expectations.

It is to be noted that the majority of license holders did not submit an STR during 2021, with the bulk of STRs being submitted by Investment Firms. Low reporting may potentially indicate weak transaction monitoring systems that are unable to detect unusual or suspicious transactions, leading to significant non-reporting of potential criminal activity. Despite there being a slight increase in the number of reports received over 2019 to 2021, STR figures are still low when compared to the number of licenced entities. As already indicated, taking a more granular look for the year 2021, one can note that the majority of STRs are emanating from investment firms, with the other licence holders each having five (5) or less STRs submitted during 2021. In this respect, at least 90% of Fund Managers, Depositaries, CISs and RFAs did not raise an STR during 2021.

Ratings are shown in the following table, that indicate that an enhancement of mitigating measures are needed specifically by the subject persons.

Table 39: Rating of effectiveness of mitigating measures – investment services sector

Mitigating measures applied at national level	
Controls applied by Supervisory Authorities in relation to licencing, supervision, enforcement, guidance, and outreach	High
Other external factors impacting the AML/CFT framework in place (participation in payment systems)	Substantial
Mitigation measures applied by Investment services sector	
Risk understanding, assessment, and management	Substantial
Customer due diligence related controls	Substantial
Resources dedicated to AML/CFT and staff knowledge (including MLROs)	Substantial
Reporting of STRs	Low

10.1.3.4 Residual risk analysis

As indicated in the below table, the overall residual risk of the sector is that of 'medium', where the residual risk is driven by ML through the misappropriation of funds, organised crime, foreign bribery and corruption, and foreign tax crime.

Table 40: Residual risk rating – investment services sector

Topic	Inherent risk	Effectiveness of mitigating measure	Residual risk level	Overall residual risk level
Misappropriation of funds	Medium-high	Substantial	Medium-high	**Overall residual risk = Medium**
Organised Crime	Medium-high	Substantial	Medium-high	
Foreign bribery and corruption	Medium-high	Substantial	Medium-high	
Foreign tax crime	Medium-high	Substantial	Medium-high	
Domestic tax crime	Medium	Substantial	Medium	
Unlicensed fund structures	Medium	Substantial	Medium	
Criminals and their associates holding or being the beneficial owner of a significant or controlling interest or holding a management function.	Medium	High	Medium-low	
Illicit use of investment securities by companies with foreign links	Medium	High	Medium-low	
ML schemes linked to customers from residence and citizenship schemes[67]	Medium	High	Medium-low	
Use of investment securities to place cash derived from proceeds of crime	Medium-low	High	Medium-low	

10.1.3.5 Recommendations

This section presents a number of recommendations to guide subject persons when applying preventative measures on a risk-based approach.

Investment service providers are to take note of the results of the NRA and, in line with their obligation at law, review and, where necessary, update, their business risk assessment and their AML/CFT framework to take into account the same.

Investment service providers are to continue investing and reviewing their AML/CFT frameworks to improve their effectiveness, including in detecting serious cases of proceeds of criminal activity to be reported to the FIAU.

Investment service providers are to ensure that adequate screening measures are implemented for a better understanding of customer risks and to ensure adequate due diligence measures are implemented. This may be especially relevant in the case where they service unregulated collective investment schemes.

[67] In the new residency by investment programme, (launched in March 2021), with regards to stock market investment, this option has been removed. The new citizenship by investment scheme programme has also removed this option.

Ensure that monitoring systems are able to detect unusual and/or suspicious transactions and activities. This may include the repeated rapid transfer, redemption and reinvestment of funds/securities, especially where these involve the sub-funds of the same collective investment scheme.

Where the investment service provider allows customers to deposit funds in an account held by the service provider, it is to ensure that funds are only used for this purpose and does not result in a situation where the service provider carries out payment services.

Ensure that sufficient mitigating measures are taken whenever investments are made in kind, including through VFAs, rather than using funds transferred through the financial system.

Undertake remedial exercises and inform the authorities about the results thereof and the measures taken to address the same.

Ensure an ongoing employee training programme.

10.1.4 Pensions services sector

The pensions services sector is composed of retirement schemes, retirement funds and related service providers, especially retirement scheme administrators (RSAs), which are subject to authorisation or licensing by the MFSA, and in the case of service providers, they are also classified as subject persons in terms of the PMLFTR. This entails that service providers are also subject to supervision by the FIAU for compliance with the AML/CFT obligations arising from the PMLFTR.

As at end of December 2021, there were 15 RSAs, 51 Schemes, divided into 45 Personal Schemes and six (6) Occupational Schemes, and two (2) Retirement Funds. Over the past years, Malta has not seen any material growth with regards to the number of licensed retirement schemes, retirement funds and related service providers, including RSAs, remaining stable. Nor has there been any material change in terms of the main form of retirement schemes, the market being dominated by Personal Schemes, i.e., retirement schemes to which individuals subscribe on their own without any contributions by employers as is the case with Occupational Schemes. On the other hand, assets under management did increase significantly. Between 2018 and 2021, there was an increase of 46% in assets under management.

The majority of retirement scheme members, almost 73% of the entire population which are on-boarded by RSAs, are British nationals. This is not surprising as the sector's primary model is aimed at the British market. The remaining 27% of the member population represent various nationalities. A similar trend has been noted with regards to the country of residence of members. Based on information collated from the pensions market, most of the members are residing in European countries, with some RSAs having about a third of their members residing in the USA and some others in non-European countries.

Furthermore, from the data collected for this sector, it has been noted that contributions generally are made from regulated pension schemes from the UK but may also take the form of in-specie transfers, a combination of in-specie and cash or cash transfers only, generally from a trust, previous pension schemes, bank accounts, savings, but also from sale of artworks. Apart from the UK, other jurisdictions from where contributions were made included other European countries as well as non-European jurisdictions, where more than 90% of the transactions as a percentage of the total population of transactions reported, are from the UK.

Subject persons are to assess their risks not only based on the analysis in their respective sectoral section, but also on additional sections, such as, the overall ML risks 'section 11', 'section 12' that presents the TF risks, 'section 13' on PF and TFS related risks, as well as the other instruments as described in 'section 9'.

10.1.4.1 ML threats

When assessing the ML threats from the data collected for this sector, it has been noted that contributions generally are made from regulated pension schemes from the UK but may also take the form of in-specie transfers, a combination of in-specie and cash or cash transfers only, generally from a trust, previous pension schemes, bank accounts, savings, but also from sale of

artworks. Apart from the UK, other jurisdictions from where contributions were made included other European countries as well as non-European jurisdictions, where more than 90% of the transactions as a percentage of the total population of transactions reported, are from the UK.

Generally, no significant changes have been noted with regards to the business models of the pensions sector. The RSAs provide retirement schemes which may be a Personal Retirement Scheme (PRS) or an Occupational Retirement Scheme (ORS) established for the principal purpose of providing Retirement Benefits.

In 2020 and 2021 there were no investigations by the Malta Police Force that had the involvement of pension funds/schemes or subject persons in the investigations that had fraud as a predicate offence. There were no international requests related to the pensions sector sent to the MTCA. However, for 2021, the ARB recorded €4.5 million frozen assets falling under the category of insurance policies, which captures both life insurance and pension plans. In essence, this includes loan protection plans used as security by banks, pension plans that need to be paid each year.

Therefore, in view of the nature of pension products, that tend to see funds inaccessible for longer periods of time and do not generally offer the level of flexibility needed to be attractive for traditional laundering of money purposes, presents a lower ML/TF threat. However, key findings presented suggest the following threats:

- Retirement schemes can at times be structured in a manner that they make aggressive use of tax arrangements or otherwise be quite complex in their set-up.
- Members' and their contributions originate from outside Malta, though mostly from reputable jurisdictions, with interaction taking place on a non-face-to-face basis.
- The nature of the scheme's members, which include what are loosely described as High Net Worth Individuals, allow for significant volumes of funds to be parked within a retirement scheme. The higher the volume of funds, the more possible that there may be co-mingled proceeds of criminal activity like tax crime.

The ratings of the ML threat assessment through this sector are presented in Table 41:

Table 41: Rating of ML threats – pensions services sector

Threat	Impact	Likelihood	Threat level
ML abuse by high-net-worth individuals	Moderate	Unlikely	Medium-low
Abuse of pension schemes for ML purposes through complex structures	Moderate	Unlikely	Medium-low
Abuse of the pension scheme sector for tax crime and related ML	Moderate	Unlikely	Medium-low
Exposure to jurisdictions: non-residents	Moderate	Possible	Medium

10.1.4.2 Vulnerabilities

This section presents the results of the assessment of the vulnerabilities in this sector, where the analysis included characteristics such as the internal governance and control set-up, business model viability, and related geographic, product and interface risks.

For example, it is to be noted that pension schemes are primarily designed for individuals which are non-Malta residents, sometimes integrated with complex structures and aggressive tax planning. This makes it difficult to understand how money is flowing, increasing the possibility that this may lead to tax crime.

A considerable amount of pension business consists of non-face-to-face transactions with initial on-boarding relying on intermediaries, both of which increase the level of ML/TF risk particularly if subject persons do not implement robust internal procedures, client on-boarding procedures, and transaction monitoring as analysed in the effectiveness of mitigating measures section.

Another vulnerability is with regards to the fact that pensions products still heavily rely on intermediaries such as Investment Financial Advisor (IFAs) or introducers to attract potential customers to become members of a personal retirement scheme. This may lead to customers being possibly entertained through multiple layers of intermediaries and the subject persons may be reliant on these intermediaries and their AML/CFT standards.

The resulting rating of vulnerabilities is presented below:

Table 42: Rating of vulnerabilities – pensions services sector

Vulnerability	Impact	Exposure	Vulnerability level
Premium relating to long-term business written via cross-border activity	Moderate	Moderately low	Medium-low
Existence of non-face-to-face transactions with initial on-boarding relying on intermediaries	Moderate	High	Medium
Business transacted via multiple layers of intermediaries	Moderate	Moderate	Medium
Reliance on intermediaries and their AML/CFT standards	Moderate	Moderate	Medium

10.1.4.3 Effectiveness of mitigating measures

The overall effectiveness of mitigating measures in the pensions services sector was found to be overall 'substantial'. The assessment took into consideration the:

- Controls put in place by regulators, namely the FIAU and MFSA, through the supervision carried out on subject persons both in terms of checks at licencing and authorisation stage to prevent the entry of bad actors in the sector as well as ongoing monitoring to ensure that subject persons are operating in line with the applicable legislative provisions.
- AML/CFT compliance programs set up by subject persons to prevent being used by their customers as a vehicle to facilitate the ML and TF.

Pensions business operating in or from Malta requires an authorisation issued by the MFSA, in terms of the Retirement Pensions Act, regulations and Pension Rules issued thereunder. The MFSA acts as the prudential regulator for the sector, whilst the FIAU is the AML/CFT supervisor.

The MFSA also acts as an agent of the FIAU in supervising the sector for AML/CFT compliance. The Insurance and Pensions Supervision at the MFSA is supported by a cross-sectoral Financial Crime Compliance Unit. The number of on-site visits carried out by the MFSA at RSAs which contained an AML/CFT element has increased significantly over 2019 to 2021. The most re-occurrent observations of these visits were:

1. Issues in relation to the MLRO demonstrating inadequate knowledge and familiarity with the AML/CFT legislative framework and implementing measures, as well as the MLRO not dedicating enough time to carry out the MLRO function in an effective manner due to other roles held. These constituted slightly more than 22% of all findings/outcomes.
2. Internal policies and procedures issues, where mainly these are either not in line with the rules and best practices, ultimately giving rise to potential systemic risk; and/or process not included in the license holder's AML Procedures Manual. These constituted slightly more than 36% of all findings/outcomes.
3. Lack of effective automated systems for monitoring customers at onboarding, policy exiting and on a continuous basis. This included automated systems lacking specific parameters such as automated customer risk assessments lacking specific parameters, constituting around 19% of all findings/outcomes.

It is to be noted however, that there were only three (3) reports received by the FIAU in 2021 from one (1) subject person. This may indicate ineffective AML/CFT compliance frameworks, and MLROs and AML teams who are unable to detect suspicious transactions.

Therefore, the ratings of this analysis are as follows:

Table 43: Rating of the effectiveness of mitigating measures – pensions services sector

Controls put in place by regulators	
Controls applied by Supervisory Authorities in relation to licensing, supervision, enforcement, guidance and outreach	High
AML/CFT controls by subject persons	
Risk Assessment and risk management	Moderate
Customer due diligence related controls (transaction monitoring included)	Substantial
Reporting of STRs[68]	Substantial
AML/CFT governance	Moderate
Resources dedicated to AML/CFT and staff knowledge (including MLRO)	Moderate

10.1.4.4 Residual risk ratings

Based on the analysis of the threats and vulnerabilities that lead to the identification of the inherent risk, and the analysis of the effectiveness of mitigating measures, it follows that the overall residual risk of the sectors is that of 'medium-low', where the residual risk is driven by the laundering of money through high-net-worth individuals, and the laundering of money through an abuse of the intermediaries and their AML/CFT structure.

[68] In view of the low amount of STRs received it is relatively difficult to make an analysis.

Table 44: Residual risk – pensions services sector

Topic	Inherent risk	Mitigating measure	Residual risk level	Overall sectoral residual risk
High-net-worth individuals	Medium	Substantial	Medium	**Overall residual risk = Medium-low**
Abuse through the reliance of intermediaries and their AML/CFT structure	Medium	Substantial	Medium	
Exposure to jurisdictions: non-residents	Medium-low	Substantial	Medium-low	
Complex structures	Medium-low	Substantial	Medium-low	
Tax crime and related ML	Medium-low	Substantial	Medium-low	

10.1.4.5 Recommendations

This section presents a number of recommendations to guide subject persons when applying preventative measures on a risk-based approach.

Primarily, pension service providers are to take note of the results of the NRA and, in line with their obligation at law, review and, where necessary, update, their business risk assessment and their AML/CFT framework to take into account the same.

Pension service providers are to continue investing and reviewing their AML/CFT frameworks to improve their effectiveness, including in detecting serious cases of proceeds of criminal activity to be reported to the FIAU.

Pension service providers that adequate screening measures are implemented for a better understanding of customer risks and to ensure adequate due diligence measures are implemented.

Ensure that monitoring systems are able to detect unusual and/or suspicious transactions and activities.

Undertake remedial exercises and inform the authorities about the results thereof and the measures taken to address the same.

10.1.5 Insurance services sector

The insurance sector in Malta which comprises of (re)insurance undertakings and intermediaries has remained fairly stable throughout 2019 to 2021 with a decrease in the overall sector population by 5%. The greatest decrease in the sector was in the number of Tied Insurance Intermediaries which decreased from 410 in 2019 to 380 in 2021. Notwithstanding this, the MFSA has continued to note interest in the insurance sector and has received new applications.

Subject persons are to assess their risks not only based on the analysis in their respective sectoral section, but also on additional sections, such as, the overall ML risks 'section 11', 'section 12' that presents the TF risks, 'section 13' on PF and TFS related risks, as well as the other instruments as described in 'section 9'.

10.1.5.1 ML threats

The analysis takes into consideration the long-term business of insurance written in or from Malta in terms of Schedule II of the Insurance Business Act. The population within the insurance sector that offer such products comprises of 12 (re)insurance undertakings and 228 Intermediaries. During 2019 to 2021, the gross written premium, for long-term business of insurance has remained relatively stable, increasing solely by around 6%. However, there has been a 27% decrease in the long-term insurance business being undertaken through agents and brokers when comparing 2019 with 2020, potentially owed to the introduction of online distribution channels.

The volume of written premium, where the country of commitment is not Malta, has increased from 2020 to 2021, with the greatest increase observed in unit-linked products. However, this has to be seen in light of the total premiums written, where it was observed that this increase was only 3% of the total written premiums in 2021 where the country of commitment is not Malta. As at the end of 2021, 45% of all long-term business constitutes of protection business, whilst around 47% relates to with-profit business, leaving a very thin share of unit-linked business being written by insurance undertakings authorised by the MFSA. No significant changes to trends have been noted when comparing the premiums written in the with-profit, unit-linked and protection business during 2019 to 2021. Whilst one notes a slight dip in protection business when comparing 2019 with 2021, which may primarily be linked to external factors such as but not limited to Covid-19 pandemic which had an indirect effect on the business models of certain insurance undertakings, there seem to be a gradual upward trend in with-profits and unit-linked business, though the underwriting of unit linked business remains relatively low being around 8% of the total written premiums.

More than 58% of the life business written by these undertakings is directed to Maltese residents. However, the long-term business offered to non-residents through freedom of service by MFSA authorised insurance undertakings is mostly protection business. It is worth noting that the protection business being written by the said undertakings is generally considered to pose a relatively low ML risk, in view of the fact that these life products are a collateral to short-term loans provided to the client by a financial institution which forms part of the same group of the insurance undertaking and are in relation to an asset (such as a motor vehicle) which is also generally bought from the same group.

Furthermore, it is to be noted that there were no international requests related to the insurance sector sent to the MTCA, and there were no STRs submitted by subject persons on the insurance sector. In 2021, four (4) subject persons within the insurance sector submitted a handful of suspicious reports to the FIAU where:

- 40% of the reports involved at least one resident in Malta
- 60% did not involve residents in Malta

In these STRs, the top predicate offences were tax crimes, and corruption and bribery.

In addition, it is to be noted that in 2021, there was one (1) ML investigation with fraud and forgery as a predicate offence that had the involvement of insurance claims fraud and the estimated amount of proceeds of crime at the initiation of the investigation was €291,000.

It is to be noted that assets analysed in this sector also featured in the assets being frozen by the ARB. In fact, for 2021, the ARB recorded €4.5 million frozen assets falling under the category of insurance policies, which captures both life insurance and pension plans. In essence this includes loan protection plans used as security by banks, pension plans that need to be paid each year.

The following table presents the results of the risk rating of the ML threats in this sector.

Table 45: Rating of ML threats – insurance services sector

Threat	Impact	Likelihood	Threat level
Exposure to jurisdictions: non-residents	Moderate	Possible	Medium
Use of illicit proceeds to purchase life insurance	Moderate	Unlikely	Medium-low
Abuse of the insurance services for fraudulent activity	Moderate	Unlikely	Medium-low
Transactions being carried out via cash or through other unregulated activity	Moderate	Unlikely	Medium-low

10.1.5.2 Vulnerabilities

The assessment of vulnerabilities mainly focused on the following categories:

- Product/interface risk - a good number of unit-linked and with-profits business allow for access to investment funds; high-value premium and overpayments; as well as transferability of the policy. In fact,
  - 45% of long-term insurance products allow for easy access to the funds, making the redemption of illicit funds to be more easily accessible.
  - 55% of products allow for high-value premium and overpayments, meaning that money launderers could potentially increase illicit money paid in terms of premium.
  - Furthermore, 64% of products allow for the transferability of the policy.
- Cross-border activity – although there has been some increase in cross border activity by some insurance undertakings offering long-term business of insurance to non-Maltese residents, the product offered are predominantly protection policies which are considered to have a low ML/TF risk.
- Business transacted via intermediaries – as within the Maltese local context, there are 20 Insurance brokers, three (3) Insurance Agents and 201 Tied Insurance intermediaries which distribute life insurance products amounting to 57%, 18% and 53% respectively, of the entire

population. However, the premiums written through such intermediaries is relatively low compared to the total premiums underwritten. This together with a reduction in the number of intermediaries offering long-term business of insurance suggests that the interface risks through intermediaries and the reliance being placed on such intermediaries for onboarding is reducing. On the other hand, there is an increased appetite for online business offerings, increasing the risk of non-face-to-face on-boarding and servicing. The vulnerability lies in the fact that there is an element of reliance on such intermediaries (including their AML/CFT standards) by the subject persons.

The result of the risk ratings is as follows:

Table 46: Rating of vulnerabilities – insurance services sector

Vulnerability	Impact	Exposure	Vulnerability level
Non-face-to-face on-boarding relying on intermediaries	Moderate	High	Medium
Reliance on the intermediaries involved in the transacted business (including in risks from transferability, easy access to funds, high premium)	Moderate	Moderate	Medium

10.1.5.3 Effectiveness of mitigating measures

Mitigating measures in place are two-fold, those implemented by insurance undertakings and intermediaries through their AML/CFT compliance programs and those implemented by the MFSA and the FIAU through checks carried out at licensing, periodic reporting requirements and ongoing supervision as well as through guidance issued on regulatory requirements and papers on typologies and red flags.

For the insurance sector, the number of on-site visits carried out by the MFSA has increased significantly from 2019 to 2021. A total number of 59 on-sites have been conducted during the period 2019 and 2021. While the visits are mostly focussed on prudential and conduct matters, these on-site visits also have AML/CFT elements, which include an interview with the MLRO. In view of the lower ML/TF risks posed by this sector in comparison to other sectors and also considering the risk-based supervisory approach adopted by local authorities, on-site visits carried out by the MFSA are the primary source to detect ML/TF red flags which filters through the FIAU's risk assessment framework, and which may trigger off further supervisory work carried out as required by the FIAU. So far, no subject person in the insurance sector has been fined by the FIAU, other than fines for late submission of regulatory returns.

Although sector-specific guidance has not been issued as of yet, general guidance issued by the FIAU applies and are equally comprehensive. Additionally, the FIAU issues typology reports and papers on red flags that are also of assistance to the insurance sector. The MFSA has also issued a number of guidance documents, including its AML Strategy[69], Guidance relating to Fit and Proper

[69] https://www.mfsa.mt/wp-content/uploads/2019/07/MFSA-AML_CFT-Strategy.pdf

Assessments[70], Guidance on Politically Exposed Persons[71], and Guidance Document to raise Awareness in relation to ML/TF risks and vulnerabilities[72]. Furthermore, the MFSA has also published a Shareholding Policy directed at credit institutions and insurance companies in 2020, setting out the MFSA's assessment of shareholding structures of credit institutions and insurance companies and also the risk appetite in relation to the assessment of shareholding structures of such entities.

The most re-occurrent observations from on-site visits were:

- Some MLRO have demonstrated inadequate knowledge and familiarity with the AML/CFT legislative provisions that need to be adhered to by subject persons, as well as not dedicating enough time to carry out the MLRO function in an effective manner due to other roles held. These constituted slightly more than 22% of all findings/outcomes. More than 19% of all recommendations which included substitution of the MLRO (around 3%) were issued by the MFSA to license holders to address this observation.
- The internal policies and procedures implemented were not comprehensive enough which prejudice the ability to implement comprehensive and effective measures to combat ML/TF risks. More than 27% of all recommendations were issued by the MFSA to license holders to address this observation.
- Lack of comprehensive measures in place for onboarding, assessing customer risks and monitoring of customer relationships. This constitutes around 19% of all findings/outcomes.

However, although there still remains room for effective implementation of AML/CFT safeguards, and despite the fact that few reports were received by the FIAU, there was an increase in 2021 of the submission of STRs by the insurance sector over the previous corresponding years. In addition, the subject persons not reporting are mainly offering loan protection covers only, so therefore the risk is lower and there is less of a chance that suspicion of ML/TF is identified in such cases.

The overall effectiveness of mitigating measures in the insurance services sector were found to be 'high'.

Table 47: Rating of effectiveness of mitigating measures – insurance services sector

Controls put in place by regulators	
Controls applied by Supervisory Authorities in relation to licensing, supervision, enforcement, guidance and outreach	High
AML/CFT controls by subject persons	
Reporting of STRs	High
Customer due diligence related controls (transaction monitoring included here)	High
Risk Assessment and risk management	High
AML/CFT governance	Substantial
Resources dedicated to AML/CFT and staff knowledge (including MLROs)	Substantial

[70] https://www.mfsa.mt/wpcontent/uploads/2019/07/20190702_FitnessPropernessGuidance.pdf
[71] https://www.mfsa.mt/wp-content/uploads/2019/04/MFSA-Guidance-on-Politically-Exposed-Persons-08-10-2018.pdf
[72] https://www.mfsa.mt/wp-content/uploads/2019/11/20191106_MFSA-Supervision-Risks-Identified-Weaknesses-And-Expected-Controls.pdf

10.1.5.4 Residual risk analysis

As indicated in the below table the overall residual risk of the sector is that of 'medium-low'. This is in view of the lower inherent risk as well as the effective mitigating measure in place.

Table 48: Residual risk ratings – insurance services sector

Threat	Inherent risk	Effectiveness of mitigating measure	Residual risk level	Overall residual risk level
Abuse of the system via the exposure to non-residency	Medium	Substantial	Medium	**Overall residual risk = Medium-low**
Abuse of the insurance services for fraudulent activity	Medium-low	Substantial	Medium-low	
Use of illicit proceeds to purchase life insurance	Medium-low	High	Medium-low	
Transactions being carried out via cash or through other unregulated activity	Medium-low	High	Medium-low	

10.1.5.5 Recommendations

This section presents a number of recommendations to guide subject persons when applying preventative measures on a risk-based approach.

Insurance Undertakings and Intermediaries considered to be subject persons in terms of the PMLFTR are to align the business and customer risk assessments as well as their AML/CFT policies and procedures with the results of the NRA.

Ensure that on a risk sensitive basis particularly on trigger events and in light with the threats prevalent in the sector, take actions to update the customer risk profiles.

Ensure the adequate consideration of risks prevalent from new onboarding methods and new payment methods in particular those related to emerging technologies and that adequate controls are implemented.

Ensure that appointed MLROs and where applicable Compliance Officers are adequately and ongoingly trained in ML/TF risks and typologies and that sufficient resources are available to be able to monitor the customer activities and transactions in line with such risks.

Take a pro-active approach to enhancing the effectiveness of AML/CFT controls and where gaps are identified implement self- imposed remedial action. Such actions are also to be communicated with the respective authorities increasing the private-public cooperation and collaboration.

10.2 Designated non-financial businesses and professions

This section presents the results of the risk assessments carried out on DNFBPs that include:

- Gaming, remote gaming operators, land-based casinos, and other land-based gaming outlets
- CSPs, accountants, auditors, lawyers, and tax advisors
- Dealing in immovable property
- Dealing in High Value Goods - Precious metals and stones, leisure yachts (greater or equal to 24 metres), luxury vehicles (greater or equal to Eur50,000), works of art and antiques, and aircraft.

Subject persons are to assess their risks not only based on the analysis in their respective sectoral section, but also on additional sections, such as, the overall ML risks 'section 11', 'section 12' that presents the TF risks, 'section 13' on PF and TFS related risks, as well as the other instruments as described in 'section 9'.

10.2.1 Gaming sector

10.2.1.1 Sector overview

The gaming sector has rapidly grown over the past twenty years. The total Gross Value Added (GVA) generated by the gaming industry during 2022 stood at €1,495 million, representing around 9.6% of the economy's GVA. When the indirect effects are included, the industry's contribution to the economic value added amounts to just over 12.4%. The gaming industry is estimated to have registered a value growth added equal to 5.8% compared to 2021. At the end of 2022, the number of companies licensed by the MGA and operating in Malta - including online and land-based entities - stood at 350. Gaming licences issued by the MGA amount to 358, as well as 329 approvals to offer various types of games under the B2C licence, and 206 approvals to offer services under the B2B licence.

The total Gross Gaming Revenue (GGR) for 2021 of B2C remote gaming operators generated from non-EU/EEA is equivalent to 35.3% of the total GGR. On the other hand, GGR generated from EU/EEA is equal to 64.7%. To further analyse the exposure of remote gaming operators to high-risk jurisdictions, an analysis of the GGR generated during 2021 was examined against the Basel AML Index, where the exposure to high-risk jurisdictions is limited at 5.4%.

Subject persons are to assess their risks not only based on the analysis in their respective sectoral section, but also on additional sections, such as, the overall ML risks 'section 11', 'section 12' that presents the TF risks, 'section 13' on PF and TFS related risks, as well as the other instruments as described in 'section 9'.

10.2.1.2 ML threats in the gaming sector

In assessing the ML threats in this sector, an analysis on the remote and the land-based casino sectors, and the recognition notice framework was carried out. Primarily, it is to be noted that in 2021, 8% of the incoming international requests received by law enforcement agencies involved

professional enablers, and half of them included gaming operators. From data shared by the MPF, between 2017 and 2019 there were 13 cases forwarded by the MGA to the MPF, the majority of which were withdrawn and not investigated further as these cases were in relation to fake websites that were taken down with no further leads being available to MPF. Furthermore, there were two (2) investigations stemming from the FIAU and reported to the MPF in the year 2019.

10.2.1.3 ML threats – Remote gaming sector

The STRs submitted by subject persons within the remote gaming and casino sectors, indicate quite a significant increase from 2018 to 2021, particularly from the remote gaming sector. When assessing the reports involving the remote gaming sector, the majority of the reports received from this sector, mainly relate to foreign nationals who have limited nexus to Malta, apart from the remote gaming account. The main predicate offences reported include fraud and tax crimes, while a good number were reported as having an unknown predicate offence. The prevalence in unknown predicate offences reporting is somewhat a given since many a time, subject persons are unable to identify predicate offences upon report submissions. Submissions are in turn primarily raised following red flags or attributes linked to a certain typology. In fact, the most common identified typology in the reports submitted throughout 2021, related to debit and credit card fraud in the case of fraud-related ML cases involving the use of remote gaming activity. In turn, the main reason for suspicion reported throughout 2021 for remote gaming operators, was the inability of the subject person to obtain sufficient corroborating evidence in relation to the players' source of wealth or source of funds. This suspicion is closely related to another commonly reported suspicion whereby the value of deposits occurring on the gaming account would not be commensurate to the players' known profile thus raising suspicion.

The following is an overview of the ML threats associated with this sector:

The use of virtual financial assets as a payment method
VFAs entail having significant elements of anonymity and a transferability element. As at end of December 2022, three (3) operators had VFA funded payments, with one operator having just been approved on 29 December 2022. Of the three (3) operators, only one (1) had 100% of their deposits and withdrawals carried out through a VFA. Deposits through VFAs for the other two (2) operators were at 1.2% and 0.2%, respectively. All three operators were operating within the ambit of the MGA Sandbox Framework which establishes several mitigating measures as will be explained in the effectiveness of mitigating measures section. In addition, it is to be noted that during the period under review for the purposes of this NRA, the MGA had already embarked on a process which then led to the publication of a policy paper on the use of DLT by authorised persons. This Policy[73] presents the MGA's position with regard to the acceptance of VFAs, virtual tokens and the use of ITAs, including DLT platforms and smart contracts, by authorised persons, and establishes further safeguards and mitigating measures and establishes that any authorised person that wishes to make use of DLT in accordance with the terms of such is required to obtain the MGA's prior approval through a specific application process.

[73] The MGA publishes its Policy on the use of Distributed Ledger Technology by Authorised Persons - Malta Gaming Authority

The use of cash as a payment method - While the use of cash is mainly associated with the land-based gaming sector, it still features minimally with remote B2C operators. The use of cash deposits with remote B2C operators was slightly over 1% in 2020, with the figure decreasing further in 2021 to 0.4%. The figure above relates to 11 unique operators that made use of cash deposits. This type of payment method is solely relevant in circumstances where remote gaming operators have physical betting shops. However, despite the relatively low percentage of cash use in this sector, cash transactions are regarded to be high risk due to the inherent anonymity of the payment method.

The use of prepaid cards and vouchers as a payment method - Similarly, to the use of cash, this payment method presents a highly anonymous means of depositing funds, as prepaid cards and vouchers can also be purchased with cash, and which can easily be exchanged or transferred between parties without controls or restrictions. Despite the anonymity factor, operators still have obligations in place to identify the player, having a registration process that is specifically dependant on such. Moreover, although in 2021 a total of 114 operators allowed the use of prepaid cards and vouchers, this payment method amounted to just over 9% of deposits made with B2C operators.

Licensed institutions controlled by foreign criminal groups - On the 22 July 2015, the Italian police had announced that an entire online network of betting companies, part of which was headquartered in Malta, had direct connections to the 'Ndrangheta', a notorious Calabrian criminal organization. As part of the operation, Italian law enforcement and prosecutors had liaised with their counterparts in Malta, which had issued Investigation and Attachment Orders on the persons and companies involved. The MGA was notified of these Attachment Orders and provided all information immediately. When the investigated persons were arrested, the MGA suspended with immediate effect the relevant licenses. The MGA had also alerted counterpart regulators in other EU jurisdictions about this case. Since then, similar accusations have reappeared in domestic and foreign media reports; however, none of which were related to persons licensed by the MGA.

Activity by un-licensed entities - Unlicensed entities pose a significant threat in terms of money laundering. These illicit operators, devoid of regulatory oversight, create an environment where funds obtained through illegal activities can be easily laundered. With little to no scrutiny on their operations, these entities can manipulate transactions, obscure the source of funds, and facilitate the integration of illicitly gained money into the legitimate financial system. The absence of licensing requirements and regulatory controls creates a breeding ground for money laundering activities, undermining the integrity of the gambling industry. The MGA's investigations team continuously conducts checks to detect activities by unlicensed entities and which are not regulated by the MGA. Any entities operating without an authorisation within Malta are also made known to the public via the MGA website. In the past, the MGA was also able to detect such through spontaneous reports submit it to it by the FIAU. In one such case, it transpired that a company was offering services which require a critical gaming supply licence from the MGA without however being in possession of such. The report was escalated to MGA's enforcement department, a 'cease and desist' letter was sent to the entity, and the case was also escalated with the MPF.

Therefore, in light of the above key findings, the rating of ML threats of the remote gaming sector, is as follows:

Table 49: ML threats - remote gaming

Threat	Impact	Likelihood	Threat level
Placement of criminal proceeds through the use of cryptocurrencies as a payment method	Significant	Possible	Medium-high
Placement of criminal proceeds through other means of payment specifically use of cash or cash facilitated payment methods	Significant	Possible	Medium-high
Licensed institutions controlled by criminals and their associates including through complex structures	Severe	Possible	Medium-high
Activity by un-licensed entities	Significant	Unlikely	Medium

10.2.1.3.1 ML threats – Land-based gaming sector

When assessing the STRs involving the land-based gaming sector, the majority of the reports received from this sector mainly relate to Maltese residents, though not necessarily Maltese nationals, and have an unknown predicate offence. Submissions are primarily raised following the identification of ML red flags or attributes with the main reason for reporting being the inability of the subject person to obtain sufficient corroborating evidence in relation to the players' source of wealth or source of funds. At times, this is also coupled with the client's lack of cooperation or outright refusal to provide information or supporting documentation.

The following is an overview of the ML threats associated with this sector:

Placement of criminal proceeds, including through smurfing and money mules, through the specific use of cash or cash facilitated payment methods
Cash, as always, remains among the most high-risk of payment methods, on the basis that cash may be freely transacted with and cash originating from ML/TF activities may quite easily be purported by the holder to be legitimate, or concealed among legitimate funds. Smurfing and the use of mules in the context of land-based operators refers to associates employed to visit land-based gaming venues to open and manage accounts with the intention to facilitate the deposit, transfer, and withdrawal of illicit funds at land-based gaming premises. The use of multiple associates (mules) would allow an individual to remain below the relevant thresholds, and therefore avoid being subjected to a client risk assessment or additional due diligence processes.

Licensed institutions controlled by criminals and their associates including through complex structures
Licensed gambling institutions controlled by criminals and their associates, often utilising complex structures, present a significant money laundering threat. While on the surface they may appear legitimate, these institutions serve as conduits for illicit funds. Criminals exploit their positions within the licensed establishments to manipulate transactions, disguise the origins of illicit proceeds, and integrate them into the formal financial system. The presence of complex ownership structures and intricate networks further complicates the detection and prevention of money laundering activities. This not only compromises the integrity of the licensed gambling sector but also poses a broader risk to the financial system by facilitating the laundering of illicitly acquired funds. Efforts to identify and dismantle such criminal control within licensed gambling institutions are crucial to combatting money laundering and preserving the integrity of the financial ecosystem.

Activity by un-licensed entities
Unlicensed land-based gambling entities pose a significant money laundering threat. Operating outside the purview of regulatory oversight, these unlicensed establishments become hotspots for illicit financial activities. The absence of proper regulations and anti-money laundering measures creates an environment where criminals can freely exploit the gambling industry for their illicit gains. Unlicensed land-based gambling entities offer anonymity and limited scrutiny, making it easier for funds acquired through illegal activities to be laundered through their operations. This poses a serious risk to the integrity of the financial system, as the lack of oversight allows the integration of dirty money into the legitimate economy. Efforts to identify and shut down these unlicensed operations are crucial to combat money laundering and protect the integrity of the gambling sector.

Therefore, considering the above key findings, the rating of ML threats of, the land-based gaming sector is as follows:

Table 50: ML threats – land-based gaming

Threat	Impact	Likelihood	Threat level
Placement of criminal proceeds through means of payment specifically use of cash or cash facilitated payment methods	Significant	Likely	Medium-high
Licensed institutions controlled by criminals and their associates including through complex structures	Significant	Possible	Medium-high
Activity by un-licensed entities	Significant	Possible	Medium-high

10.2.1.3.2 ML threats – Recognition notice framework

The Maltese recognition framework allows entities established in Malta to operate under a licence originating from another EU/EEA Member State, or non-EU/EEA jurisdictions deemed to have an AML/CFT framework and related safeguards which are considered to be "largely equivalent" to the Maltese AML/CFT Framework.

The most prevalent threats emanating from the recognition notice framework are:
- a Malta-based entity holding a licence by another EU/EEA member state (or approved jurisdiction), operating without obtaining recognition from the MGA. This is possible since notification to the MGA is not required to incorporate an entity or to obtain a foreign license. Notifying the MGA and seeking recognition is largely dependent on the operators initiating the process under the guidance of its advisors.
- a Malta-based entity that is operating under a recognition notice allowing it to operate under a less robust AML/CFT framework in respect of their non-MGA licensed activities, due to a weaker level of regulation and/or supervision in respect of the foreign licensed activities.

Therefore, in light of the above key findings, the rating of ML threats of the recognition notice framework is as follows:

Table 51:ML threats - recognition notice framework

Threat	Impact	Likelihood	Threat level
Abuse of the recognition notice framework	Significant	Likely	Medium-high

10.2.1.4 Vulnerabilities

This section presents the results of the assessment vulnerabilities for both the remote gaming sector and the land-based sector including a breakdown by every sub-sector within these two sectors. The assessment is focused on the following categories:

- Customer related vulnerabilities
- Jurisdiction related vulnerabilities
- Product related vulnerabilities
- Means of payment related vulnerabilities
- Operator AML/CFT Framework vulnerabilities

10.2.1.4.1 Customer-related vulnerabilities

Customer-related vulnerabilities are derived from customers that present a heightened level of ML/TF risk and the possibility of having customers engaging in smurfing and the use of mules as means to launder money in the gaming sector so as to divide funds and move them illicitly through networks of accounts. The customer population is virtually entirely composed of individuals and is high volume in nature. The majority of players engaging with remote gaming services are classified as low or medium risk, while PEPs pose higher risks. An understanding of the risk profile of players within the sector is key in evaluating the sector's risk drivers. Data processed analysed from the FIAU's REQs shows that 82.6% of remote gaming operators reported that high risk players constituted between 0 – 25% of their total customers, while 47.8% of operators reported that low risk players constituted between 75 – 100% of their total customers. In addition, based on the REQ analysis of all remote gaming operators, in 2022 only 3.8% of customers currently surpass the €2,000 threshold. Based on this data, 96.2% of remote gaming customers do not surpass the threshold. In turn, in 2021 land-based casinos have over 70% low-risk customers, over 20% medium-risk customers and less than 4% high-risk customers. This clearly outlines that the majority of the customer base for this sub-sector are categorized as low risk. Nevertheless, all casino licensees have at least one PEP as part of their customer base, all together amounting to a total of 138 PEPs.

Within the land-based setting, vulnerabilities stem from the potential practice of smurfing and using of mules which involves employing associates to visit land-based gaming venues to handle illicit financial transactions. These associates, or mules, open and manage accounts at the venues to facilitate the deposit, transfer, and withdrawal of funds. By using multiple mules, individuals can stay below certain thresholds, avoiding client risk assessments and additional due diligence processes. The likelihood of smurfing and mule use in land-based casinos is relatively low compared to remote gaming due to the limited number of local establishments and the requirement for physical presence, which makes it more difficult for players to exploit stolen or fraudulently obtained identities.

Other vulnerabilities stem from the organisation of junket arrangements, where such arrangements usually involve high-wealth players engaging in gambling activities with large sums of money involved. The gross revenue derived from junket arrangements fluctuates, with the percentage ranging from 3% to 18% in 2020 and from 6.0% to 52% in 2021. The increase in 2021 revenue is attributed to the easing of COVID-19 restrictions.

10.2.1.4.2 Jurisdiction-related vulnerabilities

Jurisdiction-related vulnerabilities include AML risks associated to foreign players residing in higher risk jurisdictions, risks associated to players residing in jurisdictions where gaming is illegal, and beneficial owners and/or key function holders who are citizens and/or residents in higher risk jurisdictions. The total GGR for 2021 of B2C remote gaming operators generated from non-EU/EEA is equivalent to 35.3% of the total GGR. On the other hand, GGR generated from EU/EEA is equal to 64.7%. To further analyse the exposure of remote gaming operators to high-risk jurisdictions information on the GGR generated during 2021 was examined against the Basel AML Index, which showed that the exposure to high-risk jurisdictions was limited at 5.4%.

Within a land-based setting, when land-based casinos utilise junket arrangements to attract high-rolling players, it is possible that individuals from various jurisdictions are introduced to the casino for participation in these events. There is a potential for individuals from high-risk jurisdictions to exploit the local land-based casino as a means to launder illicit funds during such events.

10.2.1.4.3 Product-related vulnerabilities

Product-related vulnerabilities include the possibility of collusion between players within the context of remote table games; transfer of funds between customers and the potential of player collusion within the context of remote P2P games; hedging opportunities and the links with match-fixing within the context of remote fixed odds betting; transfer of funds between customers within the context of remote betting exchanges; and the possibility of collusion between players and the transfer of funds between customers within the context of fantasy sports.

Players, colluding, can manipulate outcomes and transfer funds between each other. For example, online P2P games like poker provide opportunities for collusion and fund transfers disguised as winnings. Collusion practices, although possible in both remote and land-based settings, can be more prevalent in land-based casinos. Collusion can occur between players or, in rare cases, involve staff members such as dealers or floor managers. Player collusion enables activities like hedging dual-outcome events (e.g., in roulette) or transferring funds between players (e.g., in P2P poker), which can facilitate ML and TF.

Hedging bets to guarantee a return is another concern, especially in table games and fixed odds betting - whereby individuals try to limit their exposures by covering multiple outcomes for the possibility of guaranteeing a return. For example, fixed odds betting products include certain dual-outcome markets, which allow players to essentially cover both sides of the market, thereby being guaranteed a win.

Betting exchanges also present a vulnerability that enables players transferring funds to one another. A betting exchange will allow players to bet against each other, with one of the parties to

such transaction winning and the other losing. In this case players have less control over the outcome when compared to P2P poker games. Therefore, the possibility of using a betting exchange to transfer illicit funds is less likely.

Several products are fully dependent on the outcome of an underlying event. The manipulation of such events may give rise to potential ML opportunities, particularly where the customer is aware of the outcome of an event prior to such event taking place. The most obvious means of manipulating events is through match fixing in sporting events. While the sporting event is generally outside of the control of the gaming operators, knowledge of the outcome of a sporting event may lead to customers betting on a particular event and being guaranteed a winning return on such bet.

An emerging product which may also be exposed to the vulnerability of players transferring funds to one another is fantasy sports. This allows players to create a pool with the winner of the group winning the amount so pooled. However, the outcome of such is dependent on underlying live events and the pooling involved is generally very small. While exposed to fund transfers, have minimal risk due to small pools and the fact that such offerings typically take place over a prolonged period of time.

Another vulnerability within the land-based context is refining opportunities, which refers to converting low-denomination currency into higher-denomination currency particularly through slot machines. Slot machines that accept cash deposits can facilitate refining opportunities, where customers insert low-denomination notes and then withdraw the remaining balance in higher-denomination notes or as a check. This process can occur independently of casino staff members, using methods like TITO boxes. Slot and gaming machines accounted for a significant portion of real money wagers in land-based casinos. Although rare, slot machines and gaming machines can be subject to manipulation, where re-programming alters outcomes to increase the chances of winning.

10.2.1.4.4 Payment methods related vulnerabilities

Payment methods are a fundamental conduit between the player and the operator, and ultimately a pipeline for the billions of funds that are deposited, wagered, and/or withdrawn by players on the platforms of licenced operators. Therefore, operators need to ensure that their offerings facilitate and reflect the preferences of their actual and potential players.

The use of bank transfers as a payment method for remote gaming have an element of vulnerability in view of mule accounts or hijacked accounts. Gaming operators should not overly rely on banks and must exercise due diligence. Credit/debit cards can be stolen or fraudulently obtained. Fraudulent use of cards can facilitate ML, and reliance on card issuers may create gaps in controls. During 2020 bank transfers represented 37% of all deposits, whilst in 2021 this increased slightly to 39% of all deposits made. In 2020 deposits carried out through credit/ debit cards amounted to 27% of total deposits, while in 2021 this amounted to 34.7%.

Prepaid cards/vouchers and cash transactions offer anonymity and can be used to obfuscate funds for illicit purposes. Although pre-paid cards/pre-paid vouchers constitute a relatively small portion of deposits made with B2C operators, these payment methods can be described as a substitute for

cash or credit, which in turn present an anonymous means of payment that can typically be purchased in cash. In 2020 a total of 113 operators allowed the use of prepaid cards and vouchers whilst in 2021 this increased slightly to 114. Nevertheless, the use of such payment method constitutes a relatively small portion: 8.00% of deposits made with remote B2C operators during 2020, whilst in 2021 this amounted to 9.48%.

Cryptocurrencies have both advantages and present vulnerabilities. Cryptocurrencies may, as is the case for other nascent technology, be used with an illicit purpose in mind. As noted above, as at end of December 2022, only three (3) operators had VFA funded payments. Of the three (3) operators, only one (1) had 100% of their deposits and withdrawals carried out through a VFA. Deposits through VFAs for the other two operators were at 1.2% and 0.2%, respectively. In addition, all three operators were operating within the ambit and strict limitations of the MGA Sandbox Framework hence reducing the threat level from such significantly.

10.2.1.4.5 Operator AML/CFT Framework vulnerabilities

Operator AML/CFT framework vulnerabilities stem from the threat of an inadequate implementation of AML/CFT framework, that suspicious activity is not identified due to the high volume of transactions, outsourcing to third parties without the necessary safeguards, inadequate resourcing in terms of competence and/or capacity, weak AML/CFT risk culture, and failure to update internal policies and controls to mitigate the risk emanating from the launch of new offerings. With the remote gaming operators there is the vulnerability that suspicious activity is not identified due to the high volume of transactions. The nature of transactions being processed by remote gaming operators is, on average, high volume, and low value. The ability to identify suspicious activity or irregular player behaviour is highly dependent on the sophistication of technology-enabled tools, the way such tools are configured and calibrated, and the strength and skillset of the human resources responsible for identifying transactions that present a reasonable suspicion of ML/TF activity amongst a typically vast number of alerts. During 2021, there were a total of 203[74] B2C remote gaming operators with approximately 27.4 million active players. All suspicious reports received by the FIAU from the remote gaming sector were submitted by less than half of the operators. Notwithstanding the fact that these operators cover 90.3% of the market share in terms of number of players, the remaining operators that did not submit a suspicious report during 2021, collectively had 2.7 million active players.

Outsourcing certain AML/CFT activities to third parties is common among operators, but it carries an element of vulnerability if not properly governed. Operators must retain responsibility and oversight of outsourced tasks to ensure they align with company policies and expectations. The outsourcing of the business risk assessment is particularly highlighted as a potential vulnerability due to the prevalence of off-the-shelf assessments that may not adequately reflect the operator's specific risks. The sector also faces challenges in terms of resourcing qualified and experienced staff for AML/CFT compliance roles. The AML/CFT risk culture within organisations is important as lack of such is also considered to be an AML/CFT threat. There is a need for boards to prioritise AML/CFT compliance and provide sufficient budgets and resources. Reporting to the board on

[74] The 203 remote gaming operators includes all operators which had at least 1 active player or were operational during 2021.

AML/CFT issues varies among operators, and internal audit functions are not universally established.

10.2.1.4.6 Recognition notice framework

With regards to the recognition notice framework, the vulnerability lies in the fact that there is a heavy reliance on the compliance of operators to notify the MGA proactively. The absence of operator notification is challenging to identify, creating a vulnerability within the sector as the eligibility criteria established by the MGA as part of the recognition framework are completely bypassed. Furthermore, this results in an incomplete understanding of the extent of Maltese entities operating in this sector. The risk arising from reliance on foreign regulators emanates from the fact that the AML/CFT regulatory and supervisory framework of foreign regulators might not be equivalently robust as that adopted by Malta. Although EU/EEA Member States should, in principle, be bound by similar AML/CFT regulations as those applicable in Malta, the implementation and enforcement thereof may vary across Member States. As at end of 2021, 111 Malta-incorporated gaming entities were operating under a recognition notice. Of those operating under a recognition notice, 46 comprise of B2C operators.

In light of the above key findings, the vulnerability ratings are as follows:

Table 52: Rating of vulnerabilities

Remote gaming	**Impact**	**Exposure**	**Vulnerability level**
Customer related	Severe	Very high	High
Operator AML/CFT Framework	Significant	Very high	High
Jurisdiction related	Significant	Moderate	Medium-high
Means of payment	Significant	Moderate	Medium-high
Product related	Moderate	High	Medium

Land-based gaming sector	**Impact**	**Exposure**	**Vulnerability level**
Customer related	Significant	Moderate	Medium-high
Jurisdiction related	Significant	Moderate	Medium-high
Product related	Significant	High	Medium-high
Means of payment	Significant	Moderate	Medium-high
Operator AML/CFT Framework	Significant	Moderate	Medium-high

Gaming parlours	**Impact**	**Exposure**	**Vulnerability level**
Customer related	Moderate	High	Medium
Operator AML/CFT Framework	Moderate	Moderate	Medium
Jurisdiction related	Moderate	Moderately low	Medium-low
Product related	Moderate	Moderately low	Medium-low
Means of payment	Moderate	Moderately low	Medium-low

Bingo halls	Impact	Exposure	Vulnerability level
Operator AML/CFT Framework	Significant	High	Medium-high
Product related	Significant	Moderately low	Medium-low
Jurisdiction related	Moderate	Moderately low	Medium-low
Customer related	Minor	Low	Low

National lottery	Impact	Exposure	Vulnerability level
Customer related	Significant	Very high	High
Operator AML/CFT Framework	Significant	High	Medium-high
Jurisdiction related	Moderate	Moderately low	Medium-low
Product related	Moderately low	Moderate	Medium-low

Low-risk games	Impact	Exposure	Vulnerability level
Customer related	Medium	Moderate	Medium-low
Product related	Medium	Moderate	Medium-low

10.2.1.5 Effectiveness on mitigating measures in place

The assessment of the effectiveness of mitigating measures took into consideration the:

- Controls put in place by the regulator, through the supervision carried out on subject persons both in terms of the checks at licencing stage to prevent the entry of bad actors in the sector as well as through ongoing monitoring to ensure that they are operating in line with the legislative provisions.
- AML/CFT compliance programs set up by subject persons themselves to prevent them from being used by their customers as a vehicle to facilitate ML or TF.

Through joint cooperation between the FIAU and the MGA, the relevant instruments pertinent to the Sector Specific Guidance (Implementing Procedures Part II for both Land-based and Remote Gaming) are provided so that sector specific guidance to the private sector can be provided in line with the latest trends and typologies. In July 2020 the FIAU updated and revised its Implementing Procedures Part II for the remote gaming sector. This document, which may be accessed online[75], builds upon the first version which was issued in July 2018.

It is to be noted that since 2018, the Gaming sector has seen a drastic increase of STR remittance which reports were used as foundation for a strategic analysis conducted by the FIAU and key figures and observations based on 2019 STRs received from Remote Gaming Operators was published in September 2020.[76] The document details the findings of a strategic analysis on suspicious reports submitted by remote gaming licensees in Malta during 2019. Remote gaming licensees were consistently the highest reporting sector since 2019. In 2022, this is still the case. However, it is also pertinent to point out that despite remote gaming operators being subject persons since 2018, the sector still has room to improve in this regard - especially in terms of improving the quality of the STRs being reported. This is especially so, for those remote gaming

[75] https://fiaumalta.org/wp-content/uploads/2020/07/02072020_FIAU-Sector-Specific-Guidance-Document.pdf
[76] https://fiaumalta.org/wp-content/uploads/2020/09/Intelligence_Factsheet_RemoteGaming2019STR.pdf

operators from who no suspicious reports are being received but who still collectively have 2.7 million active players.

In assessing the mitigating measures for the remote gaming sector, the analysis also took into consideration the 2022 EU SNRA. While the Maltese remote gaming sector may fall under this general assessment, it is important to note that the specific risk-rating of the sector in Malta differs due to the fact that many of the controls recommended in the SNRA are already being adopted in the Maltese sector. A practical example of such is the AML/CFT risk imposed by the use of VFAs in the sector which, in the Maltese sector, is already subject to a number of controls.

Examples of mitigating measures in relation to customer-related vulnerabilities
Based on data analysed from the 2022 REQs (for end of year 2021), 97.4% of remote gaming operators have measures in place to detect the opening of multiple accounts by the same player. These measures usually detect players trying to open multiple accounts at a very early stage and are consequently restricted. In addition, as per REQ 2022 data 69.1% of the gaming operators do not have any PEPs.

Mitigating measures adopted by remote gaming operators include the adoption of identification and verification controls to detect multiple accounts and cross-check payment account holders. Customer identification and verification procedures are implemented to prevent the use of stolen or false documents. Remote gaming operators have adopted transaction monitoring systems which are sophisticated enough to continuously assess players' activity creating a risk profile on each player whilst raising an alert whenever the players deviate from their usual behaviour. In the case that an alert is raised an investigation is opened by the remote gaming operator and if grounds for suspicion remains, an STR is issued to the FIAU by the MLRO. Furthermore, the appropriate level of due diligence is kicked off once the relevant threshold of €2,000 has been exceeded as per the FIAU Implement Procedures with more onerous obligations in place when dealing with VFAs as a payment method.

Land-based casinos also have identification processes in place as per the Gaming Premises Regulations, which mandate customer identification and verification upon entrance. Casinos must also comply with various requirements, including surveillance, security, access control, and unrestricted access for Authority officers to perform inspections. The MGA also conducts thorough due diligence checks on all junket leaders. With regards to the land-based gaming sector, all four (4) subject persons carried out transaction monitoring and two (2) had the fully automated systems for monitoring transactions while another two (2) had partially automated systems. Land-based casinos also have systems in place that record and separate junket players from normal players' transactions, making it easy to reconcile at the cash desk and whenever any additional checks are deemed necessary.

Examples of mitigating measures in relation to jurisdiction-related vulnerabilities
To mitigate risks, the MGA thoroughly assesses individuals involved in the financing, investing, and management of gaming businesses. The viability of the business operation is investigated, including financial analyses, marketing strategies, and human resources plans. Operator documents and technical information are also examined. Gaming operators must comply with AML/CFT laws, determine customer risk profiles, and apply appropriate CDD measures. Risks

associated with players in jurisdictions where gaming is illegal are addressed through business plan scrutiny and the detection of illegal connections. The presence of BOs and key function holders from higher-risk jurisdictions is mitigated through controls implemented by the MBR and the MGA's vetting process. Ongoing monitoring and AML audits are performed to ensure compliance.

Furthermore, casinos are considered subject persons and are obligated to conduct the required due diligence checks. For example, casinos have multiple controls in place pertaining to junket arrangements to monitor the activity of junket players and ensure necessary checks on junket leaders, thereby limiting ML and TF vulnerabilities.

Examples of mitigating measures in relation to product-related vulnerabilities
Continuous monitoring of players' activity is a key control in effectively detecting suspicious activity, reporting such suspicion in a timely manner, and in efficiently mitigating the risk posed by product-related vulnerabilities. Remote gaming operators have adopted sophisticated tools which are constantly overseeing players activity enabling the operator to establish an accurate profile on each player. Furthermore, advanced fraud detection tools and techniques such as chat moderation are sometimes implemented to detect unusual and suspicious player behaviour. Table randomisation mechanisms are also in place to decrease the chances of two players which are known to each other to be matched and allocated to the same virtual room, hence severely minimizing the risk of collusion. Moreover, the MGA carries out system audit checks to ensure that such systems are effectively working. Therefore, although specific products offered by remote gaming operators can present players with the opportunity to collude, several targeted controls are setup to mitigate such risks from materialising.

Examples of mitigating measures in relation to payment method related vulnerabilities
Overall, examples of mitigating measures applied by the gaming sector against payment method related vulnerabilities include conducting due diligence checks, verifying the source of funds, implementing closed-loop policies, monitoring of transactions, applying information-sharing agreements with respect to PSPs, and complying with relevant regulations specific to each payment method. Specific to the risks associated with the use of VFAs as a payment method, most mitigating measures resulted from constraints imposed by the MGA Sandbox Framework, where:

- The framework delves into the verification of control over wallets, in accordance with the FIAU Implementing Procedures that are specifically applicable to the VFA sector. The wallet shall form part of the player's registered identity with an operator and in any case, control needs to be verified prior to any deposit being made from it. If control cannot be verified, pending transactions are logged and any amounts are frozen. If the player fails to verify control, the operator is obliged to appropriate such funds for responsible gaming purposes in accordance with any directions given by the MGA to this effect, without prejudice to any AML/CFT obligations.
- Moreover, the threshold for triggering CDD requirements is by far more onerous by virtue of the framework and are triggered at €150 as opposed to €2,000.
- The acceptance of VFAs which have inbuilt anonymisation functions and/or which otherwise enable the obfuscation of the address of the sender or the receiver, and/or of the amount being transferred are, by nature, incompatible with the requirements of this policy and shall be prohibited.

As indicated in the remote gaming threat assessment section, the MGA in January 2023 published its Policy on the use of Distributed Ledger Technology by Authorised Persons. In this Policy, there is specifically stated that "Authorised persons shall only engage service providers who are duly authorised in terms of the VFA Act or any other law and/or binding instrument that may be applicable in Malta from time to time." This also means that when the new rules on markets in crypto assets (MICA) come into force, said authorised persons will need to engage only service providers who are subject to such.

Examples of mitigating measures in relation to the Recognition Notice Framework
With regards to the recognition notice framework, it is important to point out that this is wholly dependent on the validity of the foreign licence. Therefore, if the foreign licence is fundamentally changed, revoked, suspended, cancelled or terminated, the recognition notice approval will cease to be valid. At application stage, the applicant is required to provide the MGA with a copy of the foreign licence, signed entity declaration form, list of games clearly showing the corresponding game type, and vertical in terms of Maltese law, letter of good standing from the relevant authority, and a legal opinion. The general terms and conditions demarcated within the recognition notice certificate establishes that this approval is issued on condition that the holder shall inform the Authority forthwith of the termination, suspension or revocation, inform the Authority forthwith to add a new licence, and subsequently add the relevant documentation, operate solely within the parameters of the approved game types/verticals. The Recognition Notice is subject to renewal every year, therefore, documents are submitted and reviewed on a yearly basis to confirm their validity.

Table 53: Effectiveness of mitigating measures - remote gaming

National controls	
Controls applied by supervisory authorities in relation to licensing, supervision, enforcement, guidance and outreach	High
By the subject persons	
Risk Assessment and risk management	High
Reporting of STRs	Substantial
Customer due diligence related controls (transaction monitoring included)	Substantial
Resources dedicated to AML/CFT and staff knowledge (including MLROs)	Substantial

Table 54: Effectiveness of mitigating measures - land-based gaming

National controls	
Controls applied by supervisory authorities in relation to licensing, supervision, enforcement, guidance and outreach	High
By subject persons	
AML/CFT governance	High
Resources dedicated to AML/CFT and staff knowledge (including MLROs)	High
Customer due diligence related controls (transaction monitoring included)	High
Risk Assessment and risk management	Substantial
Reporting of STRs	Substantial

10.2.1.6 Residual risk analysis

As indicated in Table 55, the overall residual risk rating for the remote gaming sector is 'medium', where the residual risk is driven by the risk of placement of criminal proceeds through the use of VFAs as a payment method.

Table 55: Residual ML risk rating - remote gaming

Topic	Inherent risk	Effectiveness of mitigating measures	Residual risk level	Overall residual risk level
Placement of criminal proceeds through use of VFAs as a payment method	Medium-high	Substantial	Medium-high	**Overall residual risk = Medium**
Placement of criminal proceeds through means of payment specifically use of cash or cash facilitated payment methods	Medium-high	High	Medium	
Licensed institutions controlled by criminals and their associates including through complex structures	Medium-high	High	Medium	
Activity by un-licensed entities	Medium-high	High	Medium	

As indicated in Table 56, the residual risk of the land-based gaming sector is 'medium'.

Table 56: Residual risk rating for the land-based gaming

Topic	Inherent risk	Effectiveness of mitigating measures	Residual risk level	Overall residual risk level
Placement of criminal proceeds including through use of cash or cash facilitated payment methods	Medium-high	High	Medium	**Overall residual risk = Medium**
Licensed institutions controlled by criminals and their associates including through complex structures	Medium-high	High	Medium	
Activity by un-licensed entities	Medium-high	High	Medium	

As indicated in Table 57 the residual risk rating of the recognition notice framework is 'medium-high'.

Table 57: Residual risk rating of the recognition notice framework

Topic	Inherent risk	Effectiveness of mitigating measures	Overall residual risk level
Abuse of the system through recognition notice framework	Medium-high	Moderate	Medium-high

Thus, through a weighted average analysis, the residual risk for the remote and the land-based sector is as follows:

Table 58: Residual ML risk rating by product

	Inherent Risk	Effectiveness of mitigating measure	Residual risk level
Remote Gaming Sector	Medium-high	High	Medium
Land based casinos	Medium-high	High	Medium
Linked Offerings[77]	Medium-high	High	Medium
Gaming parlours	Medium	High	Medium-Low
Low risk games – land based	Medium-Low	High	Medium-Low
Bingo halls – land based	Low	Very high	Low
National lotteries	Low	Very high	Low

A 'medium-high' residual risk lies within the recognition notice framework.

10.2.1.7 Recommendations

This section presents a number of recommendations to guide subject persons when applying preventative measures on a risk-based approach.

Recommendations to the subject persons: Remote gaming sector

Enhancing the risk-based approach, where the remote gaming operators should:
- Ensure alignment between the business risk assessment, the customer risk assessment and the findings of the NRA and periodically update the customer risk profiles.
- Review regularly the risk assessment and management processes, taking into account the contextual environment within which the activity being carried out is.
- Ensure alignment between CDD obligations and transaction monitoring, in line with the findings of the NRA.
- Continue maintaining risk-based customer due diligence policies, procedures and processes.

Monitor effectiveness of transaction monitoring systems for emerging risk, where the remote gaming operators need to:
- Have enhanced identification and verification controls in place to reduce the likelihood of individuals engaging in smurfing whilst reducing the risk of players exploiting stolen, false and/or fraudulently obtained identification documents.
- Ensure adequate maintenance and ongoing upgrades as required to their systems to facilitate screening, transaction monitoring and ensure adequate identification of suspicious transactions.
- Consider adopting data driven monitoring focusing on higher risk transactions and ensure that any suspicious transactions are escalated with the FIAU.

[77] Electronic Gaming Machines (EGMs) and Sports Betting.

Continue taking remedial action to address weaknesses in AML/CFT control framework, where the remote gaming operators should:

- Continue to take steps to assess the effectiveness of their AML/CFT control frameworks and take action to address any weaknesses identified, such as through the implementation of self-imposed remedial action plans and through cooperation with supervisory authorities to address any shortcomings identified during supervisory examinations.
- Maintain an ongoing employee training programme.

Recommendations to the subject persons: Land-based gaming sector

Enhancing the risk-based approach, where the land-based gaming operators should:

- Ensure alignment between the business risk assessment, the customer risk assessment and the findings of the NRA and periodically update the customer risk profiles.
- Review regularly the risk assessment and management processes, taking into account the contextual environment within which the activity being carried out is.
- Ensure alignment between CDD obligations and transaction monitoring, in line with the findings of the NRA.
- Continue maintaining risk-based customer due diligence policies, procedures and processes.

Monitor effectiveness of transaction monitoring systems for emerging risks, where the land- based gaming operators need to:

- Ensure adequate maintenance and ongoing upgrades as required to their systems to facilitate screening, transaction monitoring and ensure adequate identification of suspicious transactions.

Continue taking remedial action to address weaknesses in AML/CFT control framework, where the land-based gaming operators should:

- Continue to take steps to assess the effectiveness of their AML/CFT control frameworks and take action to address any weaknesses identified, such as through the implementation of self-imposed remedial action plans and through cooperation with supervisory authorities to address any shortcomings identified during supervisory examinations.
- Maintain an ongoing employee training programme.

10.2.2 Company service providers

The risk assessment on CSP (that includes trustees and fiduciaries) takes into consideration the new CSP regime following the amendments to the Company Service Providers Act[78]. The Act has introduced more onerous obligations on particularly on prudential and governance obligations. It included lawyers, notaries, auditors, and accountants within the scope of the CSP Act and service providers which were previously exempted as per the 'de minimis' rule. With this stronger regime in place, there was a decline of around 25% in the amount of CSPs being registered with the MFSA.

Subject persons are to assess their risks not only based on the analysis in their respective sectoral section, but also on additional sections, such as the overall ML risks 'section 11', 'section 12', that presents the TF risks, 'section 13' on PF and TFS related risks, as well as the other instruments as described in 'section 9'.

10.2.2.1 ML threats

Data from MFSA and from the FIAU REQs indicates that the services of a CSP are being offered by:

- 40.9% by subject persons only acting as CSP
- 22.8% operating through trustee license
- 20.4% by accountants/auditors who also have a CSP license
- 7.6% by lawyers who also have a CSP license
- 8.3% by tax advisors who also have a CSP license

Data indicates that 68% of the CSP services are being offered through legal persons (in the CSP regime referred to as 'body corporates'). Furthermore, in assessing the composition of the CSP sector by type of licenses, as at November 2022, 43.7% of CSPs have a Class C licence, where the majority of Class C licenses are held by legal persons (136 legal persons vs 48 natural persons), where this class includes the full range of CSP services, that is:

(i) formation of companies or other legal entities
(ii) provision of a registered office, a business correspondence or administrative address and other related services for a company, a partnership or any other legal entity,
(iii) acting as or arranging for another person to act as director or secretary of a company, a partner in a partnership or in a similar position in relation to other legal entities.

With regards to the jurisdictions of the BO behind those CSPs that are registered as legal persons, 42% are Maltese nationals, 31% are EU/EEA nationals, 25% are non-EU/EEA nationals and only 2% are nationals of high-risk jurisdictions.

In assessing the clients, a major threat when it comes to CSPs is the abuse of Maltese registered legal persons with no nexus to or substance in Malta for ML purposes or otherwise BO concealment. This would result in cases where a Maltese CSP is offering a registered address or has set up a Maltese legal person however there are no Maltese key officials within the legal person or otherwise the legal person is totally owned by foreigners, thus having no substantial connection with Malta. From the legal persons that were incorporated in 2020, 5,263 companies had no

[78] https://parlament.mt/en/13th-leg/acts/act-l-of-2020/

Maltese involvement except for a registered office, that is, where there is no local presence. From the legal persons incorporated in 2021, 5,760 were with no local presence, and from the legal persons incorporated in 2022, 6,150 were with no local presence.

Threats may also persist through the use of multi-national complex structures. Therefore, in the formation of new legal persons or otherwise through the usage of Maltese registered addresses, CSPs may be used in the layering stage of money laundering and to move funds through multiple entities. In complex structures, it might also be challenging to identify the ultimate beneficial owner of the entities involved, thus creating a lack of transparency. In fact, the threat of BO concealment also increases with complex structures involving multiple jurisdictions.

In 2021, there were 258 reports submitted to the FIAU from credit institutions that involved at least one Maltese legal person. This is considered to be an important aspect to take into consideration in the threat assessment for this sector in view of the fact that one of the services provided by CSPs is that of formation of legal persons. In fact, as already mentioned, data from MBR indicates that in 2021, 95% of the legal persons registered with MBR were incorporated via a CSP. From these reports submitted by credit institutions, the top indicator was that of tax crime, which featured in 77 reports. Adverse media was an indicator in 76 reports whilst transactional activity which is unexplained or inconsistent with the known customer profile was an indicator in 57 reports.

Due to the increased regulation of CSPs, individuals may also opt to set up legal persons without referring to the services provided by CSPs. This may increase the risks of Maltese legal persons being used to hold or transfer funds relating to ML/TF without the regulation of Maltese authorities. In fact, as mentioned above, whilst in 2020, 98.3% of the legal persons were incorporated by a CSP, in 2022 this percentage share declined to 91.5%.

CSPs offering directorship services or secretarial services may also lose contact with the beneficial owner during the course of the business relationship. Consequently, it may become challenging to maintain updated and correct records on the legal persons' BOs which can lead to outdated customer profiles. This may also signify potential BO concealment as it hinders the CSP from understanding whether there have been any changes in the individual(s) effectively controlling the legal person.

The following table presents the threats of ML in relation to the services offered by CSPs, in line with the PMLFTR, that include those of company formation, directorship, company secretary and registered office. The following assessment has to be seen as well together with the ML threats analysis of the legal persons section 9.1 of this document.

Table 59: Rating of ML threats - CSPs

	Impact	Likelihood	Threat level
Abuse of Maltese registered legal persons with no sufficient links to Malta for ML/TF purposes or concealment of BOs:			
When providing only services of a registered office	Significant	Very Likely	High
When providing the service of formation of legal persons or other legal persons	Significant	Possible	Medium-high
When acting as, or arranging for another person to act as, a director of a legal person	Significant	Possible	Medium-high
When acting as, or arranging for another person to act as, a secretary of a legal person	Significant	Unlikely	Medium

10.2.2.2 Vulnerabilities

Following an assessment undertaken on the CSP sector, a number of vulnerabilities have been identified, the results of which are being illustrated hereunder.

Primarily, as of November 2022, it was identified that 40.9% of CSPs are only acting as a CSP and not providing any other service, which represents an increase over the 2021 percentage share of 34%. This was considered as a vulnerability in 2021, as despite being licensed, CSP services are also being offered by unwarranted subject persons, therefore, increasing the possibility of being target for money laundering by criminals.

Also, as of 2022, the majority of CSPs (including even those acting as a CSP through the trustee license) were found to have been servicing less than 50 customers each. From the total CSPs there are only 6.7% of the natural persons that have a large client base that is more than 250 customers. From the total CSPs, there are only 12.9% of the legal persons that have a large client base, with more than 250 customers.

With regards to interface, a vulnerability identified stems from the fact that for yearend 2021, 42% of customers were onboarded by CSPs remotely. This, combined with the fact that 26% of subject persons used agents and intermediaries to onboard/service customers prompts challenges in verifying the identity of the CSPs customers and/or their beneficial owner(s).

Another vulnerability lies in the fact that in the analysis undertaken, CSPs with over than 250 customers including those registered as natural persons recorded quite a high number of customers per employee. Hence the ratio of customers to employees signifies that several CSPs lack the required resources to be able to effectively manage its customers and ensure it is not being used for the purpose of facilitating ML/TF.

Through the latest FIAU REQs for this sector, it was identified that when assessing the service of directorship services 25% of the individual CSPs offer directorship services to more than 20 companies. This may indicate a lack of proper oversight in view of the number of companies being serviced. Another vulnerability is in relation to the multiple services being offered by the CSPs to

the same customer for example, directorship services, secretary, and registered address, which albeit enabling more oversight and understanding of customer compared to provision of one service only, it may lead to cases of inadequate identification of the beneficial ownership.

Throughout the review, an ML/TF risk was identified within the CSP sector stemming from when a company's share capital is paid through pooled accounts. Using pooled accounts to pay a company's share capital can make it difficult to trace the original source of funds. Hence, money launderers may exploit this anonymity to introduce illicit funds into the system through the company by commingling them with legitimate funds from other investors. This can obscure the true origin of the funds and allow illicit money to enter the company undetected.

Another vulnerability is the lack of visibility by a Maltese CSP on their customers' activity due to such companies operating overseas and having a limited local footprint, as well as the fact that in Malta there is a relatively high number of Maltese companies which are owned by foreign individuals. These scenarios increase the possibility of potential offshore tax crime, i.e., setting up a company in a jurisdiction with no connection to the company's actual operations. Such companies may also be used to engage in cross-border transactions for the purposes of the movement of illicit funds or the disguise of activities. This would make it more difficult to identify and investigate the flow of illegitimate funds.

Furthermore, there can be the vulnerability in relation to exemptions in the licensing regime, where for example, CSP services to listed or MFSA licensed entities, such CSPs limiting their services to such entities are excluded from authorisation requirements under the CSP Act which implies that therefore these are not subject persons. The supervision on licensed CSPs: listed or MFSA-licensed entities are excluded from reviews of CSP's client files, as CSP has no AML/CFT obligations with respect to the said customers. The ML/TF risks are mitigated on the basis of (i) the scrutiny that would have accompanied the entity at authorisation stage; and (ii) with respect to licensed entities, they are themselves subject in most cases to AML/CFT requirements and therefore subject to supervision by FIAU and MFSA. The working paper for this sector contains a section that details the justifications for the exemptions and explains why these are not constituting a vulnerability for this sector.

A summary table with the rating of key vulnerabilities that lead to a further exploitation of the assessed ML threats, is as follows:

Table 60: Rating of vulnerabilities - CSPs

	Impact	Likelihood	Threat level
Share capital of established legal persons can be paid through pooled accounts	Severe	High	High
Conducting CDD and having all relevant documentation in the absence or a limited local footprint	Significant	Very high	High
Relatively high number of foreign-owned legal persons	Significant	Moderate	Medium-high

10.2.2.3 Effectiveness of mitigating measures

In 2019, the MFSA embarked on a project to 'raise the bar' with respect to those persons offering CSP services. Amendments to the Company Service Providers Act removed the previous exemption from licensing for lawyers, notaries public and other legal professionals when these perform CSP activities. Act L of 2020[79] was approved by Parliament and published on the 13 November 2020. These amendments provided for the following:

- Inclusion of lawyers, notaries public, auditors and accountants, within scope of the CSP Act and subject to adequate market entry requirements and proportionate ongoing fitness and propriety and compliance requirements.
- Including service providers that are currently exempt under the "de minimis" rule within the scope of the CSP Act and the market entry requirement and making them subject persons; and
- Strengthening the ongoing requirements applicable to CSPs with regard to Governance, Risk Management, Compliance and Time Commitment addressing relevant outcomes of the sectoral risk assessment.

Thus, prior to the new CSP licensing regime, a number of professionals (such as warranted lawyers and accountants) and individual service providers providing directorship and company secretary services below certain thresholds were exempt from MFSA licensing. Through legislative amendments published in 2020, these have now also been captured within the MFSA's licensing and supervisory remit, and therefore required to undergo the same fitness and propriety assessments as well as ongoing scrutiny by the MFSA. With this amendment there is a harmonisation of the market entry requirements and reducing and eliminating existing gaps, increased AML/CFT oversight by both competent authorities working jointly, as well as increasing enforcement action through sanctioning or remediation plans, depending on the severity of the breaches identified.

As part of the MFSA's supervision of these subject persons, the regulatory frameworks require that these have in place adequate systems and controls which should cover also record keeping requirements and ensuring compliance with AML/CFT legislation thereby reducing the potential threat of ML/TF. Hence, with the new CSP licencing regime applicable as from May 2021, this implied that all CSPs are now subject to robust fitness and properness checks (both at authorisation stage and also ongoing).

In view of such changes, during phase 1 of the new CSP regime there were 77 withdrawals (individuals and entities) both voluntary and forced withdrawals. Out of these 77, 29 were forced withdrawals whereby following an assessment the MFSA deemed that the applicant does not have the necessary set up to operate adequately. In phase 2 there were a further 29 withdrawals, 20 were voluntary and the remaining lapsed by operation of law. This data is linked exclusively with the applications brought about through the new CSP regime. Therefore, data is now available on previously unregulated population or else which used to be regulated only from an AML/CFT supervisory perspective. This enhances the implementation of the multi-pronged approach and enables enhanced risk-based supervision.

[79] https://parlament.mt/en/13th-leg/acts/act-l-of-2020/

It is in breach of law to offer CSP services without having obtained/applied for a license. To effectively monitor this, the MFSA and MBR have an arrangement in place whereby MBR checks whether the person incorporating a company/offering registered office/being appointed director/company secretary has been authorised by the MFSA or is currently being processed as a provisionally authorised CSP. In default, the MBR would stop such individual/entity, and where necessary refer to the MFSA for possible investigation of unlicensed activity.

Data by the FIAU shows that there was an increase in supervision on CSPs by 211% in the three-year period July 2019 to June 2022 when compared to the previous three years (2016-2018). This was also a result of an increase in FIAU resources dedicated to DNFBPs supervision section (3 personnel in 2018 which increased to 6 in 2022). With regards to supervision on CSPs, by 2022, 81% of the high-risk categorised subject persons undergone a compliance review. Apart from the increase in the AML/CFT supervisory coverage, the period 2019 to 2022 has also experienced an increase in the number of dissuasive enforcement measures being applied by the FIAU on subject persons that fail to adhere to AML/CFT obligations following a compliance review. This since as at year end 2022, a total of 26 CSPs were fined in total of €604,199 (2020 - €278,022; 2021 - €97,500; 2022 - €228,677), this along with the imposition of 20 Directives for CSPs to remediate their identified shortcomings. Despite the enforcement action taken by the FIAU, it is important to also keep in mind the vulnerabilities in the legal system impacting the dissuasiveness of enforcement measures for breaches of AML/CFT obligations. Also, there was more guidance and outreach in the past three years from the FIAU (15 guidance documents issued, 18 training events organised and 350 queries answered).

With regards to STR reporting by the CSPs, there was an increase in the number of the STRs between 2018 to 2021. The number of STRs submitted by the CSPs continued to increase from 2019 to 2021. However, only a part of the subject persons actually reported STRs, where it is to be noted that the majority of the non-submitters from the CSPs are subject persons that service less than 20 customers, and therefore, given that they are smaller firms their risk appetite is less, or they operate a low-risk business model and therefore, they would be less likely to come across suspicious activity. In addition, when assessing the follow-up to the reports those that led to an outcome were minimal, thus indicating lower quality STRs, thus highlighting a need for improvement in the reporting of the STRs.

Pertinent findings from recent REQ data are that for example, a number of subject persons providing CSP services seem to be reliant on the fact that transactions will be monitored by other subject persons (such as credit institutions/financial institutions) with the result that such subject persons were sanctioned for these failures.

The resulting effectiveness of controls is as follows, where moderate improvements are required on risk-based supervision, minor improvements with regards to enforcement, guidance and outreach, and the fitness and proper checks. With regards to the AML/CFT controls by the subject persons, major improvements are needed with regards to risk assessment that will further lead to a higher quality of STRs.

Table 61: Rating of the effectiveness of mitigating measures - CSPs

Controls put in place by regulators	
Controls applied by Supervisory Authorities in relation to licensing, supervision, enforcement, guidance and outreach, fitness and proper checks	High
AML/CFT controls by subject persons	
Reporting of STRs	Moderate
Customer due diligence related controls (transaction monitoring included here)	Substantial
Risk Assessment and risk management	Substantial
AML/CFT governance	High
Resources dedicated to AML/CFT and staff knowledge (including MLROs)	High

10.2.2.4 Residual risk analysis

This section presents the residual risk ratings per threat assessed in the services offered by the CSPs to legal persons that are registered in Malta. As shown in the below table, the overall risk rating for the services offered by a CSP is 'medium-high', which has to be seen in line with the 'medium-high' residual risk rating in the legal persons' sector. For example, as detailed in the legal persons' risk assessment, the fact that the majority of the high-risk legal persons registered at the MBR do not have a Maltese IBAN account indicates a lower risk of abusing the Maltese financial system for laundering the foreign proceeds of tax crime by legal persons that are registered in Malta, but this also indicates that the main gatekeepers to mitigate the risk of misuse of legal persons for foreign tax crime purposes are the CSPs.

Table 62: ML Residual risk analysis - CSPs

Topic	Inherent risk	Effectiveness of mitigating Measure	Residual risk	Overall residual risk level
Abuse of Maltese registered legal persons with no sufficient links to Malta for ML/TF purposes or concealment of BOs:				
When providing only services of a registered office	High	Moderate	High	**Overall residual risk = Medium-high**
When providing the service of formation of legal persons	Medium-high	Substantial	Medium-high	
When acting as, or arranging for another person to act as, a director of a legal person	Medium-high	High	Medium	
When acting as, or arranging for another person to act as, a secretary of a legal person	Medium	High	Medium-low	

10.2.2.5 Recommendations

This section presents specific recommendations to guide the CSPs when applying preventative measures on a risk-based approach.

CSPs are to align the business and customer risk assessments as well as their AML/CFT policies and procedures with the results of the NRA.
Periodic risk sensitive reviews of the policies and procedures in place.

Ensure that on a risk sensitive basis particularly in line with the threats prevalent in the sector, actions are taken to update the customer risk profiles.
CSPs should be able to demonstrate the application of risk-based customer due diligence.

Take a pro-active approach to enhancing the effectiveness of AML/CFT controls and where gaps are identified take actions aimed at increasing self- imposed remedial actions.
Such actions are to be encouraged to be communicated with the respective authorities increasing the private-public cooperation and collaboration.

10.2.3 Accountants and auditors

This section presents the results of the risk assessment carried out on assessing the misuse of accountants and auditors for ML purposes.

Subject persons are to assess their risks not only based on the analysis in their respective sectoral section, but also on additional sections, such as the overall ML risks 'section 11', 'section 12', that presents the TF risks, 'section 13' on PF and TFS related risks, as well as the other instruments as described in 'section 9'.

10.2.3.1 ML threats

Data from the supervisory authorities indicates that the population of accountants and auditors that offer only one relevant activity and that are registered with the FIAU has increased from 2020 to 2021. The share of the subject persons registered at the FIAU as accountants and auditors that offer more than one relevant activity stands at 23.2% of the accountants and auditors registered with the FIAU. In addition, the majority of the accountants and auditors are natural persons.

It is to be noted that with regards to the services offered by the accountants and auditors that offer no other service, other than a relevant activity, the highest service being offered is that of audit and assurance. In this category the accountants and auditors that are mostly legal persons account for 33%. This is followed by the preparation of the financial statements where again the majority of such service is being offered by legal persons.

Furthermore, it is to be noted that the majority of the accountants and auditors that conduct only one relevant activity that falls under the PMLFTR, have less than 50 customers. Out of the accountants and auditors registered as natural persons, only 2% of such have 250 or more customers, whereas there are 15% of the accountants and auditors registered as legal persons that have 250 or more customers. Furthermore, a more in-depth analysis of the granular data indicates that the natural persons have higher number of customers per employee than those accountants and auditors registered as legal persons.

With regards to ML investigations in 2021, there were four (4) ML investigations with the involvement of one (1) accountant and five (5) auditors. In these investigations, typologies identified were:

- Bank accounts used as conduit
- Use of foreign legal persons
- Self-Laundering and third-party laundering
- Laundering through car dealing, drug trafficking, tax crime
- Not declaring the total income
- Laundering proceeds trough gambling
- Failure to submit the audited financial statement and annual returns to the MBR
- Front organization
- Opening of local legal persons
- Cash deposits and cheque deposits while declaring with unemployment
- Income being declared does not correspond with cash deposits in personal account

- Smurfing
- Fake invoicing

With regards to prosecutions, out of a total of 55 ML prosecutions in 2021, in 21 prosecutions, there was the involvement of 24 natural persons and 14 legal persons. From these 21 prosecutions there was also the involvement of nine (9) professional enablers of which there were four (4) accountants, two (2) auditors, and one (1) audit firm.

Taking into account these key findings and output of the sectoral working groups that included the private sector representatives, the resulting ratings of the assessment of the ML threats from accountants and auditors is as follows:

Table 63: Ratings of ML threats - accountants and auditors

Threat	Impact	Likelihood	Threat level
Failure to identify money laundering:			
Audit and assurance	Severe	Possible	Medium-high
Assisting in the planning and carrying out of transactions	Severe	Possible	Medium-high
Preparation of financial statements	Significant	Unlikely	Medium
ML through liquidation of legal persons	Significant	Very unlikely	Medium

10.2.3.2 Vulnerabilities

This section presents the results of the assessment of the vulnerabilities for subject persons providing accounting and auditing services, where the focus mainly is in relation to the main vulnerabilities that are linked to the absence or a limited local footprint in Malta.

Table 64: Ratings of vulnerabilities - accountants and auditors

Vulnerability	Impact	Likelihood	Vulnerability level
Audit and assurance – Conducting CDD and having all relevant documentation in the absence or a limited local footprint	Significant	Moderate	Medium-high
Preparation of financial statements: Verifying the information in the absence or a limited local footprint	Significant	Moderately low	Medium
In course of liquidation: Potential manipulation by cooperation between creditors and liquidated legal persons	Significant	Low	Medium

10.2.3.3 Effectiveness of mitigating measures

This section presents the ratings of the effectiveness of mitigating measures, which include the national controls and the controls applied by the accountants and auditors. It is to be noted

primarily that auditors are subject to quality assurance checks. Accountants are also subject to mandatory Certified Public Accountant (CPA) and submission of annual return.

The Accountancy Board carries out risk intelligence screening by means of a reputable international database together with searches on the internet. The majority of applications received by the Accountancy Board meet the above-mentioned requirements and the applicants are issued with a CPA warrant and or a PCA. However, over the last five (5) years the Accountancy Board refused nine (9) applications:

- four (4) of which did not meet the qualifications requirements as stipulated in sub-article 3(2)(c) of the Accountancy Profession Act,
- while the other five (5) applications did not meet the work experience requirements namely in the case of applications for a CPA warrant where the applicants did not satisfy the Board that they have adequate experience in the practice of accountancy for an aggregate period of three years, while in the case of applications for a PCA the applicants did not satisfy the Board that they have gained the equivalent of three years full time practical training in inter alia auditing of financial statements, at least two-thirds of which shall be with an auditor approved in any Member State.
- Two (2) of the applicants who did not meet the qualifications requirements lodged an appeal with the Administrative Review Tribunal, both cases are still ongoing.

In addition, data by the FIAU shows that there was an increase in supervision by 211% in the three-year period July 2019 to June 2022 when compared to the previous three years (2016-2018). This was also as a result of an increase in FIAU resources dedicated to DNFBPs supervision (3:2018 and 6:2022), which led to an increase in examinations held from seven (7) in 2021 to 35 in 2022.

Apart from the increase in the AML/CFT supervisory coverage, the period 2019 to 2021 has also experienced an increase in the number of dissuasive enforcement measures being applied by the FIAU on accountants and auditors, being subject persons that fail to adhere to AML/CFT obligations. Enforcement measures include both pecuniary fines as well as other administrative measures including the imposition of remediation directives for subject persons to address gaps in their AML/CFT control framework. Whilst pecuniary fines aim to dissuade gatekeepers from breaching AML/CFT obligations, follow-ups carried out by the FIAU on remediation directives served are intended to ascertain that such subject persons successfully implement the remedial action to address gaps in their AML/CFT compliance programs.

With regards to ML/TF reporting by accountants and auditors to the FIAU, both registered an increase in the reports submitted from 2018 to 2021. However, it is to be noted that only 9% of accountants and auditors are actually reporting a STR to the FIAU. Furthermore, it is to be noted that a number of the STRs submitted had an insufficient element of ML/TF and ended with no disseminations/further action.

The following table presents the ratings for the effectiveness of mitigating measures. This indicates that moderate improvements are needed in relation to the risk-based supervision. In this regard, it is important to highlight that in December 2022, the FIAU being the sole AML/CFT regulator in Malta issued the Part II of the FIAU Implementing Procedures for Accountants and Auditors, which are binding procedures on all accountants and auditors to follow in adhering with their

AML/CFT obligations. The said Implementing Procedures Part II came into force in April 2023. Major improvements are needed with regards to the risk understanding and risk assessments that can in turn lead to an improvement in the overall quantity and quality of STRs submitted by this sector.

Table 65: Ratings of the effectiveness of mitigating - by accountants and auditors

Controls put in place by regulators	
Controls applied by Supervisory Authorities in relation to licensing, supervision, enforcement, guidance and outreach, fitness and proper checks	Substantial
AML/CFT controls by subject persons	
Reporting of STRs	Moderate
Customer due diligence related controls (transaction monitoring included here)	Moderate
Risk Assessment and risk management	Substantial
AML/CFT governance	High
Resources dedicated to AML/CFT and staff knowledge (including MLROs)	High

10.2.3.4 Residual risk analysis

As shown in the following table, the overall residual risk rating for the services provided by accountants and auditors is 'medium', with the residual risk driven by the services in relation to the 'audit and assurance' and the 'assisting in planning and carrying out of transactions'. Here the mitigating measures are not robust enough in view of the vulnerabilities in relation to the challenge in verifying and having all documentation in the absence or a limited local footprint as also evidenced in the legal persons' risk assessment.

Table 66: Residual risk ratings - accountants and auditors

Topic	Inherent risk	Effectiveness of mitigating measure	Residual risk	Overall residual risk level
Laundering of money through:				
Audit and assurance	Medium-high	Substantial	Medium-high	**Overall residual risk = medium**
Preparation of financial statements	Medium	High	Medium-low	
Liquidation	Medium	High	Medium-low	

10.2.3.5 Recommendations

This section presents recommendations to guide subject persons when applying preventative measures on a risk-based approach.

Accountants and auditors are to *take note of the results of the NRA* and, in line with their obligation at law, *review and, where necessary, update*, their business risk assessment and their AML/CFT framework to take into account the same.

Accountants and auditors are to *continue investing and reviewing their AML/CFT frameworks* to improve their effectiveness, including in detecting suspicions of proceeds of criminal activity to be reported to the FIAU.

Monitor the effectiveness of transaction monitoring systems for national and emerging risks
Accountants and auditors should assess and monitor the effectiveness of their transaction monitoring measures and align to the recent Implementing Procedures to ascertain that these allow proper detection of transactions that may be related to national or emerging risks. Accountants and auditors should also ensure that assessment of the effectiveness of their transaction monitoring system also takes into consideration the submission of good quality and material STRs.

10.2.4 Lawyers

Lawyers providing specific professional legal services are considered to be subject persons carrying out relevant activity as per the PMLFTR. These services involve assisting clients in transactions involving the buying or selling of real estate or business entities; liquidation of companies; assisting in the planning or carrying out of transactions for clients concerning the organization of contributions necessary for the creation, operation, or management of companies; assisting in the planning or carrying out of transactions for clients concerning the opening or management of bank, savings, or securities accounts; and assisting in planning or carrying out of transactions for clients concerning the managing of client money, securities, or other assets. A risk assessment was carried out on lawyers carrying out these types of activities.

Subject persons are to assess their risks not only based on the analysis in their respective sectoral section, but also on additional sections, such as the overall ML risks 'section 11', 'section 12', that presents the TF risks, 'section 13' on PF and TFS related risks, as well as the other instruments as described in 'section 9'.

10.2.4.1 ML threats

Data from the FIAU REQs indicates that the number of customers serviced by lawyers decreased by 53% in 2021. Furthermore, whereas the percentage of lawyers incorporated as legal persons decreased from 55% in 2020 to 44% in 2021, the share of natural persons carrying out the activity increased from 45% in 2020 to 56% in 2021.

The most common relevant activity carried out in 2021 was assisting clients in transactions involving the buying or selling of real estate or business entities with 41% of total relevant activity. Services in relation to assisting in the planning or carrying out of transactions for clients concerning the organization of contributions necessary for the creation, operation or management of companies, accounted for a share of around 20% out of the total relevant services provided by lawyers, while around 7% of relevant activity involved assisting in the planning or carrying out of transactions for clients concerning the opening or management of bank, savings or securities accounts. Around 4% of relevant activity involved assisting in the planning or carrying out of transactions for clients concerning the managing of client money, securities and other assets, while only around 28% of all relevant activity involved the liquidation of companies. Thus, the 'assisting in the planning or carrying out of transaction' function in line with regulation 2 of the PMLFTR accounted for a total share of 31.3%, composed of

- 20%: assisting in the planning or carrying out of transactions for clients concerning the organization of contributions necessary for the creation, operation, or management of companies
- 7%: assisting in the planning or carrying out of transactions for clients concerning the opening or management of bank, savings, or securities accounts, and
- 4%: assisting in planning or carrying out of transactions for clients concerning the managing of client money, securities or other assets.

In terms of customers being serviced by subject person lawyers who are natural persons and who offer no other relevant activity, 94% fall within the category of 'very small' i.e., having less than

50 customers. 4% of customers of the same category of lawyers fall within the category of 'small' with customers ranging between 50 and 149 in number, while 1% of such customers fall within the 'medium' range with 150 to 249 customers.

Likewise in the category of lawyers who are legal persons and who provide no other relevant activity, 92% of customers are 'very small' with less than 50 customers, while the remaining 8% of the customers services by such category of subject persons are 'small' with a number of customers between 50 and 149. Furthermore, it is to be noted that the number of customers serviced by lawyers decreased by 53% in 2021from 2020.

When assessing the ML investigations and prosecutions, it is to be noted that in 2021, two (2) ML investigations involved a lawyer in each case, while ML prosecutions in the same year involved nine (9) professional enablers, of which one (1) was a lawyer.

In assessing the rating of the ML threats, the analysis focused on the services provided by subject person lawyers, that is,

- Assisting in transactions involving the buying or selling of real estate or business entities
- Liquidation of companies
- Assisting in the planning or carrying out of transactions for clients concerning the organization of contributions necessary for the creation, operation, or management of companies
- Assisting in the planning or carrying out of transactions for clients concerning the opening or management of bank, savings, or securities accounts
- Assisting in planning or carrying out of transactions for clients concerning the managing of client money, securities, or other assets.

Taking into account these key findings and output of the sectoral working groups that included the private sector representatives, the resulting ratings of the assessment of the ML threats from lawyers is as follows:

Table 67: Rating of ML threats - lawyers

Threat	Impact	Likelihood	Threat level
Failure to identify money laundering in:			
Transactions involving the buying or selling of real estate or business entities	Significant	Possible	Medium-high
The planning or carrying out of transactions for clients concerning the organization of contributions necessary for the creation, operation, or management of legal persons	Significant	Possible	Medium-high
The planning or carrying out of transactions for clients concerning the opening or management of bank, savings, or securities accounts	Significant	Unlikely	Medium
The planning or carrying out of transactions for clients concerning the managing of client money, securities, or other assets	Significant	Unlikely	Medium
Liquidation of legal persons	Significant	Unlikely	Medium

10.2.4.2 Vulnerabilities

The vulnerabilities presented here are in relation to the services provided by the lawyers, focusing on vulnerabilities in relation to:

- Lack of sufficient due diligence if and when pooled accounts are used.
- Lack of sufficient information as to the company's actual activity when it is a foreign customer.
- Challenge of verifying information regarding foreign beneficial owners.
- Challenge of ongoing monitoring when company activity is outside Malta.

Table 68: Rating of vulnerabilities - lawyers

Vulnerability	Impact	Exposure	Rating level
Share capital of established legal persons can be paid through pooled accounts	Severe	Moderate	Medium-high
Verifying, identifying and ongoing monitoring when servicing clients in the absence or a limited local footprint	Significant	Moderate	Medium-high

10.2.4.3 Effectiveness of mitigating measures

This section presents the ratings on the effectiveness of mitigating measures with the overall rating of 'substantial'. Data by the supervisory authorities indicates that there are no high-risk subject persons under this category and that between July 2019 and June 2022, the FIAU carried out examinations on 20% of subject person lawyers.

The number of reports submitted to the FIAU by lawyers increased from 10 in 2019 to 25 in 2020 and decreased to 15 in 2021. The 2021 figures implies that only 5% of the subject persons reported an STR. Furthermore, out of the STRs submitted in 2021 there were 31% of the STRs submitted by this sector that had insufficient elements with no disseminations, thus indicating a lower quality element.

The ratings of the effectiveness of mitigating measures are indicated in the table below, where moderate improvements are needed on the monitoring upon obtaining the warrant stage and the fitness and proper checks in the absence of a warrant. Minor improvements are needed by the supervisory authorities in terms of guidance and outreach. With regards to the AML/CFT controls by subject persons, major improvements are needed in relation to the governance, risk assessments and risk understand that would in turn lead to a higher quantity and higher quality STRs.

Table 69: Effectiveness of mitigating measures - lawyers

Controls put in place by regulators	
Level of dissuasiveness of final enforcement measures after appeal for breaches of AML/CFT obligations, AML/CFT guidance and outreach, level of AML/CFT supervision, national cooperation between the authorities, fitness and proper checks.	Substantial
AML/CFT controls by subject persons	
Reporting of STRs	Moderate
Customer due diligence related controls	Substantial
Risk understanding, assessment and management	Substantial
Resources dedicated to AML/CFT and staff knowledge (including MLROs)	Substantial

10.2.4.4 Residual risk analysis

The overall residual risk rating of the lawyers' sector is 'medium'. The drivers of the risk rating are attributable to the services of assisting in transactions involving the buying or selling of real estate or business entities and assisting in the planning or carrying out of transactions for clients concerning the organisation of contributions necessary for the creation, operation, or management of companies. This has to be viewed with particular reference to the 'medium-high' residual risk rating attributed to the real estate sector, and the 'medium-high' residual risk rating in the legal persons' sector.

Table 70: Residual risk rating - lawyers

	Inherent risk	**Effectiveness of mitigating measure**	**Residual risk**	**Overall residual risk level**
Laundering of money through:				
Buying or selling of real estate or business entities	Medium-high	Substantial	Medium-high	**Overall residual risk = Medium**
The planning or carrying out of transactions for clients concerning the organization of contributions necessary for the creation, operation, or management of legal persons	Medium-high	Substantial	Medium-high	
The planning or carrying out of transactions for clients concerning the opening or management of bank, savings, or securities accounts	Medium	Substantial	Medium	
Planning or carrying out of transactions for clients concerning the managing of client money, securities, or other assets	Medium	Substantial	Medium	
Liquidation of the legal persons	Medium	High	Medium-low	

10.2.4.5 Recommendations

This section presents key recommendations to guide lawyers when applying preventative measures on a risk-based approach.

Lawyers are to *align the business and customer risk assessments* as well as their AML/CFT policies and procedures with the results of the NRA. This should allow for the implementation of risk based due diligence measures.

Enhancing the risk-based approach
Lawyers are encouraged to update their business risk assessment and customer risk assessment methodology to take into account the results of the NRA.

Better awareness of ML/TF indicators
Lawyers should increase their knowledge and awareness in relation to identifying red flags indicating a suspicious act of ML or TF. Such knowledge and awareness should assist in increasing the quantity of STRs submitted to the FIAU. They should also engage in further training and guidance so as to improve the quality of STRs submitted.

10.2.5 Tax advisors

Maltese law does not provide a definition of the activity or activities that would fall to be considered as tax advice. In an effort to facilitate the conduct of the NRA, the following services were considered to fall within the wider category of tax advice:

- Advice on the legitimate minimization of tax burdens
- Corporate re-organization
- Transfer/Sale of on-going concerns
- Repatriation of assets
- Succession and estate planning
- Re-domiciliation of entities
- Advice on specific tax related questions, tax audit, tax planning or tax optimization
- Cross border tax advisory services

In addition, the provision of tax advice in Malta is not subject to any *ad hoc* regulation, including market entry requirements. Nevertheless, as explained further hereunder, the vast majority of persons engaged in the provision of tax advice are in practice, accountants, auditors or lawyers. These professionals are subject to regulation as well as other market entry requirements including fitness and properness checks. However, it is still the case that any person may hold him/herself out to offer tax advice services.

Subject persons are to assess their risks not only based on the analysis in their respective sectoral section, but also on additional sections, such as the overall ML risks 'section 11', 'section 12', that presents the TF risks, 'section 13' on PF and TFS related risks, as well as the other instruments as described in 'section 9'.

10.2.5.1 ML threats

Data from the supervisory authorities indicates that overall, the number of customers being serviced by the tax advisors has decreased by 17% from 2020 to 2021. The service of tax advice is being provided by:

- 49% by accountants and auditors,
- 29% by CSPs,
- 6% by lawyers,
- 3% by trustees and fiduciaries, and
- 13% by a category that offers exclusively tax advice and with no other relevant activity.

The last category does not necessarily mean that they are non-warrant holders and unregulated, but it is likely to be the case. The absence of market entry controls creates a number of difficulties, including, among others, the challenge it poses for authorities to have a full picture of the population of this sector, and to therefore ensure that the sector is adequately guided and supervised for AML/CFT purposes.

From those subject persons providing tax advice, 67% are legal persons and 33% are natural persons. In the case of legal person CSPs, legal person accountants and auditors (accountancy and audit firms), and legal person lawyers (law firms), the majority of such subject persons service

more than 250 customers. Those subject persons that offer tax advice only (i.e., the 13%) service less than 50 customers, and are considered to be 'very small' subject persons.

The main services offered by tax advisors are:

- Advice on the legitimate minimization of tax burdens. This accounts for the highest share of services provided – at 67%
- Corporate re-organization – which accounts for 12% of the services offered; and
- Advice on specific tax related questions, tax audits, tax planning or tax optimization – which accounts for 9.1% of services provided.

The inherent threat being assessed here is in relation to providing advice on tax and cross-border related questions, tax audit, tax planning or tax optimization being misused by someone to justify a ML scheme. Taking into account these key findings and output of the sectoral working groups that included the private sector representatives, the resulting ratings of the assessment of the ML threats from tax advisors is as follows:

Table 71: Rating of ML threats - tax advisors

Threat	Impact	Likelihood	Threat level
Advice on tax and cross-border related questions, tax audit, tax planning or tax optimization being misused by someone to justify a money laundering scheme	Significant	Very likely	High

10.2.5.2 Vulnerabilities

The key vulnerabilities in this sector are in relation to:

- Lack of *ad hoc* market entry requirements, including fitness and properness checks for tax advisors
- Lack of sufficient guidance on international illegitimate tax planning which leads to a vulnerability in relation to the extent of understanding international fiscal complexities
- Lack of sufficient data on the number of tax advisors
- Lack of sufficient guidance on the various topics addressed in this profession that is, repatriation of assets and estate planning for example.

The vulnerabilities presented here are in relation to the services provided.

Table 72: Rating of vulnerabilities - tax advisors

Vulnerability	Impact	Exposure	Vulnerability level
Lack of sufficient guidance on various topics, including on international illegitimate tax planning	Severe	Very high	High
Lack of sufficient data on the sector	Significant	High	Medium-high
Lack of licensing regime for tax advisors	Significant	Moderately low	Medium

10.2.5.3 Effectiveness of mitigating measures

The overall effectiveness of mitigating measures in this sector was found to be 'moderate'. Within the context of the provision of tax advice, the lack of market entry controls is considered to present a higher weight in the inherent risk analysis, for which there is not an effective mitigating measure other than the fact that very few unregulated or unwarranted natural persons and/or legal persons actually provide tax advice.

In addition, the number of reports submitted by the tax advisors to the FIAU in 2021 amounted only to very few reports, also implying that only 1% from this category of subject persons reported to the FIAU in 2021. The examinations carried out by the FIAU from 2019-2021 covered 27% of the registered population as tax advisors with the FIAU.

The following table presents the effectiveness of mitigating measures.

Table 73: Rating of effectiveness of mitigating measures – tax advisors

Controls put in place by regulators	
Limited AML/CFT supervision, guidance and outreach, national cooperation between the authorities, fitness and proper checks	Low
AML/CFT controls by subject persons	
Reporting of STRs	Low
Customer due diligence related controls	Moderate
Resources dedicated to AML/CFT and staff knowledge (including MLROs)	Moderate

10.2.5.4 Residual risk analysis

The following table presents the residual risk analysis of the advisors, where the overall residual risk rating is 'medium-high'. This residual risk is driven mainly by the risk of laundering from the advice on the legitimate minimization of tax burdens, the advice on specific tax related questions, tax audit, tax planning or tax optimization, and the cross-border tax advisory services. While this is not necessarily and specifically linked to the laundering of foreign tax crime, the fact that Malta's income tax regime is at risk of being misused to launder the proceeds of crime, was considered of relevance to the tax risk assessment carried out in 2021, where the key findings are publicly available on the NCC website[80].

[80] RESOURCES - NCC (gov.mt)

Table 74: Residual risk analysis - tax advisors

Topic	Inherent risk	Effectiveness of mitigating measures	Residual risk	Overall residual risk level
Abuse of tax advice services for ML purposes with lack of commercial rationale by				
Advice on specific tax related questions, tax audit, tax planning or tax optimization	High	Low	High	**Overall residual risk = Medium-high**
Cross border tax advisory services	High	Low	High	
Corporate re-organisations	Medium-high	Substantial	Medium-high	
Repatriation of assets	Medium-high	Substantial	Medium-high	
Succession and estate planning	Medium-high	Substantial	Medium-high	
Transfer / Sale of ongoing concerns	Medium	Substantial	Medium	
Re-domiciliation of entities	Medium	Substantial	Medium	

10.2.5.5 Recommendations

This section presents recommendations for the tax advisors (including the subject persons that do not offer exclusively tax advice) with the objective of addressing the key vulnerabilities and the key drivers of the residual risk analysis.

Enhancing the risk-based approach
Tax advisors are encouraged to update their business risk assessment and customer risk assessment methodology to take into account the results of the NRA.

Better awareness of ML/TF indicators
Tax advisors should increase their knowledge and awareness in relation to identifying red flags indicating a suspicious act of ML or TF. Such knowledge and awareness should assist in increasing the quantity and quality of STRs submitted to the FIAU.

10.2.6 Immovable property, real estate agents and notaries

Transactions in the immovable property sector are facilitated by a range of service providers including notaries who execute and register immovable property sale deeds; real estate agents who act as intermediaries between buyers and vendors; banks who provide credit facilities to finance immovable property acquisitions; and lawyers who may be involved in immovable property related transactions. Therefore, this chapter should be read in conjunction with the other chapters relating to other services to understand how money can be laundered through the immovable property sector.

This chapter addresses the risk of dealing with immovable property related transactions and distinguishes between two main subject persons involved, that is, the notaries and real estate agents. It is to be noted that although immovable property sales have experienced a 16% decline between 2019 and 2020, during the year 2021 sales have increased by 29% over the previous year, reaching a total of 14,436 immovable property acquisitions.

Subject persons are to assess their risks not only based on the analysis in their respective sectoral section, but also on additional sections, such as the overall ML risks 'section 11', 'section 12', that presents the TF risks, 'section 13' on PF and TFS related risks, as well as the other instruments as described in 'section 9'.

10.2.6.1 ML threats

Immovable property acquisition is an attractive method for criminals to hide their illicit proceeds since, although the movement of funds is relatively slow, criminals can launder large amounts of money in one transaction. Furthermore, there is a year-on-year appreciation trend in property valuation and criminals may also invest in property to rebuild and sell at a higher price with the objective of justifying their income. Although the scale of money laundering through the property sector is unknown, the share of real estate assets frozen in Malta in 2021 was estimated at 75% (€44.6m), thereby indicating that money laundering through the real estate sector is significant. In all cases where there was the freezing of the immovable assets, the majority of cases had no involvement of foreigners. In addition, the analysis of STRs submitted in relation to this sector indicate that the majority of the reports had at least one Maltese resident involved, whereby the attributable predicate offences were mainly domestic tax crimes. During 2021, there were eight (8) ML investigations that involved three (3) subject persons, highlighting the risk that gatekeepers may also end up assisting in the facilitation of ML.

During the three-year period ending 31 December 2021, acquisition of real estate property by foreigners did not register an increase, and Maltese nationals accounted for 98% of the property deeds acquired.

The acquisition of property through the use of legal persons is seen to carry a higher degree of risk in comparison to buyers who are natural persons, since the former may, albeit not necessarily, create challenges in determining the beneficial owners. However, an analysis of property deeds registered in 2019, 2020 and 2021 indicates that the overwhelming majority of buyers are natural persons (92% - and almost entirely Maltese nationals), whereas legal persons accounted for 8%.

An analysis of the nationalities of the BOs of legal persons involved in the acquisition of immovable properties indicates that that the greatest part (90%) of the legal persons owning such immovable property are BOs who are Maltese nationals and that such legal persons did not form part of complex structures. As for the remaining 10%, 7% were nationals from EU countries and only 3% were third country nationals.

During 2021, a total of 52 properties were purchased for a value exceeding €2 million, 52% of which were made by Maltese nationals and 48% by legal persons, where the BOs are also Maltese nationals. This analysis also indicates that in terms of legal persons, real estate property is mainly acquired by Maltese residents and beneficial owners of Maltese nationality – and not through complex structures owned by individuals residing in high-risk jurisdictions.

The First Time Buyers Scheme offered by the Maltese Government for the past years, which is applicable only to Maltese buyers purchasing their first residential property contributes to the large proportion of Maltese nationals buying property. This Scheme accounts to 20% of property deeds. UK and Chinese nationals accounted for 35% of the foreign buyers during this period.

Although the Use of Cash (Restriction) Regulations which came into force in March 2021 has mitigated the risk of cash derived from illicit proceeds from being used to purchase property, the Regulations do not extend to the use of cash for construction, renovation or finishings and therefore the risk that cash from criminal activities is laundered in the property sector. Similarly, there is also the risk that cash derived from illicit sources may also be used to lease property, particularly if the monthly rent amounts to less than €10,000 since this falls outside the scope of the PMLFTR.

In the property sector, there are instances where sellers and buyers may attempt to reduce their taxes dues on property transfers by deliberately undervaluing the properties. According to data from the MTCA, in 2021, there were 4,550 cases of potential undervaluation, which constituted 32% of all purchase deeds during that year. However, in cases where MTCA identifies potential undervaluation, action is taken accordingly through the appointment of an independent architect who, following re-valuation of the property, the buyer would be obliged to pay tax accordingly on the re-valued property.

The resulting ratings for ML threats are shown in the table that follows, where it should be noted that the risk of abuse of services provides by notaries are real estate agents are assessed separately since their roles in immovable property transactions are significantly different. Subsequently, there is a different likelihood that the abuse materialises.

As explained in Cap 615 (2020) Real Estate Agents, Property Brokers and Property Consultants Act, 'real estate agent' means any natural person who has a licence to act as an intermediary in the process of negotiating and arranging transactions involving the acquiring or disposing or leasing of land and employs and, or engages (whether under a contract of service or a contract for services) one or more branch managers and, or one or more property consultants. Generally, the real estate agent would personally meet both the vendors and the buyers prior to the execution of sales transaction. In the Maltese context, the real estate agent does not hold any client monies until such time that the property acquisition transaction is finalised. In fact, it is typically the notary who is entrusted to retain any deposit paid by the buyer upon signing of the promise of sale in a clients'

account. This deposit is held by the notary until searches on the property's legal status are concluded by the latter and the deed of sale is signed by the vendor, the buyer and the notary. Furthermore, the deposit typically exceeds €10,000 and is in bank draft or cheque form. The notary is also responsible to ensure that the deed of sale is registered and taxes due are paid accordingly to the MTCA. Therefore, from the real estate agent's perspective, the threat of abuse for ML through property acquisitions is limited given that the real estate agent has a licence to act only as an intermediary in the process of negotiating and arranging transactions involving the acquiring or disposing or leasing of land.[81]

Table 75: ML threats – immovable property, real estate agents and notaries

Threat	Impact	Likelihood	Threat level
Use of immovable property acquisitions to launder the proceeds of domestic crime	Severe	Likely	High
Tax offences related to the purchase of immovable property transfers including by undervaluation	Significant	Possible	Medium-high
Notaries' services abused for ML through property acquisitions	Significant	Possible	Medium-high
Real estate agents' services abused for ML through property acquisitions	Significant	Very unlikely	Medium
Laundering of proceeds of crime through the purchase of real estate by legal persons including through complex structures	Significant	Unlikely	Medium
Laundering through the use of cash in mortgage loan repayments, leasing, renovation or finishings	Significant	Unlikely	Medium
Laundering the proceeds of foreign crime in Malta through the acquisition of immovable property	Significant	Unlikely	Medium

10.2.6.2 Vulnerabilities

A vulnerability exists with regard to the limited scope of the PMLFTR regarding real estate agents' sales offices operated by employees of contractors in Malta involved in some of the sales of the real estate in the jurisdiction. Immovable property sales that are facilitated through employees of contractors. Since the latter are not considered as subject persons, CDD checks are not carried out in the same manner as those implemented by real estate agents. Notwithstanding this, all property deeds are subject to CDD checks by notaries, and no property transactions where there is the transfer of immovable property, or any real right over immovable property may be executed without the involvement of a notary.

In addition, further to the Act[82] regulating the Real Estate Agent, Property Broker, Branch Manager & Property Consultant that came into force on the 3 July 2020, a legal notice was issued obliging

[81] For risks relating specifically to the CBI/RBI schemes see 'section 9.3'.

all interested parties within the sector to register their intention by end of March 2021 and subsequently to apply for a license to operate in the sector by end of December 2021. To date, there was no enforcement to those operating without a license and a vulnerability lies with regards to the exemption article 3, sub-article 3 that states:
'No licence shall be required where a person acts as an intermediary in the process of negotiating and arranging transactions involving the acquiring or disposing or leasing of land on an occasional basis and does neither advertise his services nor does he employ or engage anyone to assist him in the carrying out of the said occasional activity.' where, as stated in article 4*: "occasional basis" means acting as an intermediary in the process of negotiating and arranging not more than two (2) transactions per annum involving the acquiring or disposing or leasing of land.'*

The overall vulnerabilities assessed were rated as follows:

Table 76: Rating of vulnerabilities – immovable property, real estate agents and notaries

Vulnerability	Impact	Exposure	Vulnerability level
Lack of sufficient AML/CFT knowledge for the real estate agents/agencies	Significant	Moderate	Medium-high
Property sales facilitated by employees of property developers not subject to CDD checks (apart from CDD checks by notaries)	Significant	Moderate	Medium-high
Exemption in legislation regarding real estate agents	Significant	Moderately low	Medium

10.2.6.3 Effectiveness of mitigating measures

The assessment of the effectiveness of mitigating measures takes into consideration the controls applied at a national level, particularly by regulatory authorities, as well as controls put in place by notaries and the real estate agents.

An important legislation that enhanced the effectiveness of mitigating measures in the immovable property sector is the Use of Cash (Restriction) Regulations[83] which came into force in March 2021. These Regulations prohibit the use of cash payments for certain high-value goods including immovable property. It is however to be noted that as at date of publication of the NRA no enforcement measures have been applied. Notwithstanding this, through the public awareness campaigns launched by the FIAU in this context, there is now a good level of awareness amongst notaries and real estate agents that cash payments over €10,000 to acquire immovable property are illegal. Furthermore, through data gathered by the FIAU through the submissions of REQs by notaries, it resulted that a significant number of immovable property acquisitions are financed through a bank loan, and therefore such transactions are also subject to CDD checks by local credit institutions.

[83] LEĠIŻLAZZJONI MALTA (legislation.mt)

In the immovable property sector, where the purchasers are foreign nationals, notaries also distinguish between those coming from an EU Member State and those who come from outside the EU (third country nationals). The law in place that guides notaries as to whether or not a notary needs to apply for a special permit (AIP permit), when it comes to the acquisition of immovable property, is Chapter 246 of the Laws of Malta, namely the Immovable Property (Acquisition by Non-Residents) Act. When the purchasers are entitled to acquire immovable property without an AIP permit, it is obligatory for the purchasers to declare this fact on the deed of purchase and for the notary to record this declaration.

As from 1 January 2022, persons acting as real estate agents require to be licenced by the Licensing Board in terms of the Real Estate Agents, Property Brokers and Property Consultants Act (Chapter 615 of the laws of Malta). Since the introduction of this Act, real estate agents are now subject to fit and proper checks. However, cross-checks carried out between the FIAU and the Licensing Board revealed that a number of real estate agents have not yet informed the FIAU that they are providing relevant activity, and are therefore not yet subject to AML/CFT supervision by the FIAU, which weakens the effectiveness of this mitigating measure.

On the other hand, data from the Notarial Council indicates that the total number of practising notaries in 2021 is at par with the FIAU data.

Further, the FIAU has increased its AML/CFT supervisory interventions on notaries and real estate agents and has also issued guidance on risk factors, mitigating measures and red flags in the property sector.

During the past few years, notaries are increasingly outsourcing the implementation of CDD procedures to AML/CFT consultants, which, in general, has led to an increase in the quality of CDD measures applied in this sector. Notwithstanding this, the application of the risk-based approach in the carrying of CDD measures is an area for improvement, since supervisory examinations carried out by the FIAU has revealed instances were CDD measures applied are not modified/intensified in the case of higher-risk occasional transactions. Conversely, the FIAU has also identified various instances where due diligence carried out was excessive when compared to the risk of ML/TF.

In the case of real estate agents, these do not typically outsource CDD procedures. Supervisory examinations carried out by the FIAU indicate that, in general, there is a lower level of AML/CFT awareness among real estate agents operating individually rather than as an agency employing several real estate agents. This is mainly because the former deal with a lower volume of immovable property acquisition deeds, sometimes also relying on the CDD checks conducted by other subject persons involved in the transaction, such as notaries or banks.

During 2021, a total of 26 and 20 STRs were submitted by notaries and real estate agents respectively, with the total STR submission representing 0.32% of the total number of property deeds in the same year. A higher proportion of STRs is expected.

The resulting ratings are as follows:

Table 77: Rating of effectiveness of mitigating measures – immovable property, real estate agents and notaries

Controls put in place by regulators - notaries	
Controls applied by supervisory authorities in relation to authorisation, supervision, enforcement, guidance and outreach	Substantial
Controls put in place by regulators – real estate agents	
Controls applied by supervisory authorities in relation to licensing, supervision, enforcement, guidance and outreach	Moderate
AML/CFT controls by notaries	
Reporting of STRs	Moderate
Customer due diligence related controls	Substantial
Risk understanding, assessment, and management	Substantial
Resources dedicated to AML/CFT and staff knowledge (including MLROs)	Substantial
AML/CFT controls by real estate agents	
Reporting of STRs	Moderate
Customer due diligence related controls	Moderate
Risk understanding, assessment, and management	Moderate
Resources dedicated to AML/CFT and staff knowledge (including MLROs)	Moderate

10.2.6.4 Residual risk analysis

As indicated in the below table the overall residual risk of the sector is that of 'medium-high'. This residual risk rating is driven by the domestic side of the laundering of money. This is sustained by the fact that the highest category of buyers of the high-end property are Maltese nationals or Maltese beneficial owners of the Maltese registered legal persons.

Table 78: Residual risk table – immovable property, real estate agents, and notaries

Topic	Inherent risk	Effectiveness of mitigating measures	Residual risk	Overall residual risk level
Laundering the proceeds of domestic crime including tax crime, through the acquisition of immovable property	High	Substantial	Medium-high	**Overall residual risk = Medium-high**
Tax offences related to the purchase of real estate property transfers including by undervaluation	High	Substantial	Medium-high	
Laundering through the use of cash in mortgage loan repayments, leasing, renovation or finishings	Medium-high	Moderate	Medium-high	
Notaries' services abused for ML through property acquisitions	Medium-high	Substantial	Medium-high	
Real estate agents' services abused for ML through property acquisitions	Medium	Moderate	Medium	
Laundering of proceeds of crime through the purchase of real estate by legal persons including through complex structures	Medium	Substantial	Medium	
Laundering the proceeds of foreign crime in Malta through the acquisition of immovable property	Medium	Substantial	Medium	

10.2.6.5 Recommendations

This section presents recommendations to guide subject persons when applying preventative measures on a risk-based approach.

Enhancing the risk-based approach
Notaries and real estate agents should align the business risk assessment and the customer risk assessment with the results of the NRA and take steps to carry out CDD procedures that reflect the risk identified in relation to occasional transactions carried out. The enhanced risk understanding will allow them to carry out better risk-based mitigating measures that address the type of risk identified.

Better awareness of ML/TF indicators
Notaries and real estate agents should increase their knowledge and awareness in relation to identifying red flags indicating a suspicious act of ML or TF, such as those noted from the behaviour of the parties to a contract. Such knowledge and awareness should assist in increasing the quantity of STRs submitted to the FIAU.

Licensed real estate agents
The notaries as subject persons are to start collecting the data regarding the involvement or non-involvement of a licensed or non-licensed real estate agent.

10.2.7 Dealing in high-value goods

This section presents the findings of the risk assessment assessing the ML threats and vulnerabilities of luxury movables being used to launder the proceeds of crime, including in the art world and the marketplaces for leisure yachts, precious stones and jewels, high-end apparel and accessories, vehicles and the aviation sector, and the high value dealer involved in the buying and selling of any of these goods in the ordinary course of their business. Certain high value goods such as luxury watches, motor vehicles and boats are particularly attractive to criminals as both lifestyle goods and economic assets. There is no universally recognised definition of a 'high-value good'. In this NRA the focus is on the sectors identified in the Use of Cash Restrictions Regulations (S.L. 373.04). Through these Regulations, it is now a criminal offence to make or receive payment or carry out a transaction in cash amounting to €10,000 or more (or its equivalent in another currency), whether in a single transaction or in several linked transactions. This restriction applies only in respect of the sale or purchase of any of the following:

- antiques
- immovable property
- jewellery, precious metals, precious stones and pearls
- motor-vehicles
- sea-craft
- works of art

In line with the above context, the high-value movables and dealers covered include:

- Works of art and antiques
- Precious metals and stones
- Luxury vehicles (greater or equal to €50,000)
- Leisure yachts (greater or equal to 24 metres)

Aircraft is also analysed here, and the ML threats in relation to immovable property are assessed in section 10.2.6.

Subject persons are to assess their risks not only based on the analysis in their respective sectoral section, but also on additional sections, such as the overall ML risks 'section 11', 'section 12', that presents the TF risks, 'section 13' on PF and TFS related risks, as well as the other instruments as described in 'section 9'.

10.2.7.1 ML/TF/PF/TFS threats

This section presents a general overview of the sectors to provide context in the analysis of the threats. In carrying out the analysis overall there was insufficient data as to the specific threats of the sector in Malta, and the analysis relies on the inherent threat, the findings of the EU SNRA, and known typologies from the case studies and quantitative information that were made available by the competent and law enforcement authorities.

Overall, high-value goods featured in a minor share of the total suspicious reports received by the FIAU in 2021. The reports included mainly motor vehicles, followed by precious metals and stones, and a number of leisure yachts. In 2021, the FIAU also received a handful of international

requests for information or spontaneous intelligence reports from foreign FIUs that involved high-value goods.

Key contextual factors of the high-value goods being taken into consideration are:

Works of art:
- As at 2022 there were 15 licensed auctioneers with their correspondence address being in Malta. Data from the National Statistics Office outlines that the auctioneers' activity and work of arts as a percentage of GDP remained relatively stable for retail sale of second-hand goods in stores, whereas other retail sale in new goods in specialised stores fluctuated from 0.9% in 2016 to 1.05% in 2020.
- Data on the imports of works of art indicates that the imports for 2021 increased significantly compared to previous years from €3.8 million to €22.1 million.
- With regards to the country of origin of the imports, 1.6% are from EU countries and the rest are from non-EU countries. From this share of non-EU countries, 58.9% originate from the European Free Trade Area.
- With regards to freezing of assets, works of art accounted for a minor share of the movable assets that were frozen, where for example, with ML stand-alone cases, works of art accounted for 0.2% of the movables, with ML with tax crime as a predicate offence, works of art accounted for 0.5% of the movables confiscated, and in ML with a predicate offence of fraud, works of art accounted for 0.3% of the movables confiscated.

Precious metals and stones:
- From data shared by the MBR and the Commerce Department, as at 2021 there were 336 dealers in precious metals and stones (DPMS) in Malta. The majority are sole traders, and a small share is exclusively foreign owned.
- Turnover of the DPMS declined from around 1.6% of GDP to around 0.1% of GDP in 2020.
- The major source market of imports of diamonds is the EU, however an increase in imports from Africa can be noted in 2021.
- Precious metals and stones accounted for 13.4% of the moveables that were confiscated in 2020, while in 2021 this accounted for only 0.005%.

Luxury vehicles:
- There are 74 car dealers selling new cars of which only a handful have a foreign nationality but reside in Malta.
- 308 car dealers sell used cars which are all resident in Malta, with a handful that are foreign nationals. A cross-check with the MTCA revealed that from this figure of 308 car dealers, unique identifiers amount to 145 car dealers, where out of these 145 car dealers, 44 are inactive.
- In 2021, the percentage share of the vehicles of a selling price of €50,000 and above[84] out of the stock of licensed motor vehicles in Malta stood at 0.9%.
- Vehicles with a selling price of €50,000 or higher accounted for 1.2% as a share of the passenger cars.
- Out of the newly registered vehicles with Transport Malta in 2021 with a selling price equivalent to or higher than €50,000 at the point of registration:

[84] Excluding the categories in relation to government owned vehicles or agricultural related, coaches and private buses, minibuses or buses, special purpose vehicles or road tractors

  - 17.4% were categorised as 'used' whereas
  - 82.6% were categorised as 'new'.
- From the analysis of the data available on car dealers, it could be observed that the majority of vehicles having a registered value higher than €50,000 are under the name of a handful of dealers.
- It is also to be noted that a number of high valued vehicles are being leased, where here it is to be noted that leased vehicles are operational and therefore there is no supervision at all on the monthly cash payments made to the car dealer.
- A number of vehicles featured as moveable assets in freezing orders by the ARB in 2021.

Leisure yachts:
- In 2021, data from the Shipping Registry on the ownership of nautical vehicles indicates that there are 6,058 nautical vehicles registered with the Maltese flag, where:
  - 1,981 were legal persons that own a nautical vehicle
  - 4,077 were natural persons that own a nautical vehicle

- A more granular analysis of the register indicates that:
  - Of the 1,981 legal persons, 1,411 have a Maltese registered company (71.2%)
  - Of the 4,077, there are 3,612 Maltese nationals (88.6%). Then 1,411 are registered in the name of Maltese registered legal persons, and 17% are foreign owned. Out of this 17%, 9% are registered legal persons and 8% are registered in the name of foreign natural persons, with the major source markets being Italy, UK and Germany.
  - Out of these nautical vehicles, 27% are leisure yachts.
  - Out of these leisure yachts, 52% are registered under a Maltese registered legal persons and an analysis by residency and nationality of the BOs of such legal persons revealed that there are a few BOs from high-risk jurisdictions.
  - For the analysis of ML threat, it is indispensable to distinguish between the different types of leisure yachts including fishing boats, commercial yachts, leisure yachts that had registered under the leasing scheme. The ML threat is more pronounced with the chartering activity that can only be offered by those registered as commercial, and especially where the activity is outside Malta in view of the lack of controls applicable.
  - Incoming international requests to MTCA involved three (3) requests in 2019 and one (1) in 2020 received from EU jurisdictions, however no fraudulent activity was detected.
  - Data on the freezing of assets reveal that in 2020 there was one nautical vehicle frozen having a value of €400,000.

Aircrafts:
- Analysis of the BOs of legal persons registered as aircraft owners in Malta revealed that there were occasions where BOs had exposure to jurisdictions in close proximity to sanctioned countries.

Further to these key findings, the ratings of ML threats for this sector are as follows:

Table 79: ML/TF/PF/TFS threats – dealing in high-value goods

Threat	Impact	Likelihood	Threat level
Laundering of domestic proceeds from the acquisition of high-value motor vehicles, including through the use of cash and/or instalments	Significant	Very likely	High
Leisure yachts as part of VAT fraud	Significant	Possible	Medium-high
Acquisition of leisure yachts including concealment of BO and / or through chartering	Significant	Likely	Medium-high
Concealment of ownership of motor vehicles[85]	Significant	Likely	Medium-high
Laundering through the precious metals and stones	Significant	Unlikely	Medium
Concealment of ownership of aircraft registered in Malta[86]	Significant	Unlikely	Medium
Laundering of foreign proceeds through the acquisition of high-value motor vehicles	Significant	Unlikely	Medium
Laundering through auctioneers and works of art	Moderate	Unlikely	Medium-low

10.2.7.2 Vulnerabilities

This section presents the ratings of the assessment of the vulnerabilities. A specific vulnerability for the leisure yachts is in relation to the fact that for an international owner, a resident agent resident in Malta needs to be appointed which are normally CSPs. The vulnerability is that the provision of resident agency services is not an AML/CFT regulated activity. Legal or accountancy professionals who act on behalf and for their client in a financial transaction are however required to carry out AML/CFT obligations. Nonetheless, it is questionable whether the activities of resident agents, even when performed by lawyers or accountants, constitute the representation of clients in financial transactions since resident agents are not involved in the brokering of the actual vessel acquisition but they represent the client vis-à-vis registration filings with Transport Malta. Furthermore, there is no effective tool or system to ensure that a person/company providing resident agent services to non-Maltese legal persons (international owner) owning a yacht or vessel under the Maltese flag, is in fact capable of, or qualified to act in this capacity.

In addition, the limited controls at some entry points, especially with regard to intra Schengen movement, is another added vulnerability, together with the added vulnerability of limited search capabilities in some of the registries.

Overall, the assessed vulnerabilities are the following:

[85] Including through hire purchase agreement or leasing.
[86] Any concealment in relation to other legal persons refer to 'section 9' on other instruments.

Table 80: Vulnerabilities– dealing in high-value goods

Vulnerability	Impact	Exposure	Vulnerability level
Limited visibility of activity of leisure yachts registered in Malta sailing abroad	Significant	Moderate	Medium-high
Limited controls especially with regard to intra Schengen movement at some of the entry points	Significant	Moderate	Medium-high
Provision of resident agency services is not an AML/CFT regulated activity	Significant	Moderate	Medium-high
Limited search capabilities in some of the registries	Significant	High	Medium-high
Lack of monitoring over chartering and leasing activities	Significant	High	Medium-high

10.2.7.3 Effectiveness of mitigating measures

This section presents the ratings of the assessment of the effectiveness of mitigating measures that take into consideration both the national controls and the controls by the sector. In the analysis of the effectiveness of mitigating measures there was missing information, and this is especially in view of the fact that 'The Use of Cash (Restrictions) Regulations (S.L. 373.04)'[87] only came into force in March 2021. In fact, as a result of this restriction, in Malta, dealers in high value goods are subject to AML/CFT obligations and supervision

(i) in the case of art galleries, auctioneers and freeports that act as traders or intermediaries in the sales of works of art, when they are involved in a transaction of €10,000 or more

(ii) in the case of freeports when these store works of art the value of which exceeds €10,000.

The Use of Cash (Restriction) Regulations (S.L. 373.04) that came into force in March 2021 led to several actions by the supervisory authority in order to have all the framework in place to monitor and enforce these Regulations. Therefore, following the introduction of these Cash restriction Regulations, the necessary guidance, policies and procedures, and awareness campaigns were introduced, with the necessary resources as well set up.

Since 2018 only three (3) reports were submitted to the FIAU by dealers in precious metals and stones. This is indicative of a total absence of reporting awareness within the analysed sectors. It is to be noted that as of 1 January 2021, a licence is required to carry out trade in precious metals and stones in line with the provisions of Trading Licences (Amendment) Regulations (L.N. 261 of 2020).

It is to be noted that with respect to the leisure yachts purchased via a registered mortgage, only 17% of those registered as commercial boats and 1.8% of the pleasure boats have a registered mortgage. Thus, registered mortgage as a mitigating factor is rather limited in nature in view of the low number.

[87] LEĠIŻLAZZJONI MALTA (legislation.mt)

The level of effectiveness of mitigating measures in this sector is rated as 'substantial'. Moderate improvements are needed with regards to risk-based supervision and major improvements are needed in relation to the enforcement for non-compliance with the Cash Regulations. Major improvements are also needed in relation to risk understanding and assessment by the subject persons that will in turn impact positively the quantity and quality of reports sent to the FIAU.

Table 81: Rating of the effectiveness of mitigating measures – dealing in high-value goods

Controls put in place by regulators	
AML/CFT guidance and outreach, level of AML/CFT supervision, national cooperation between the authorities, fitness and proper checks	Substantial
AML/CFT controls by subject persons	
Reporting of STRs	Low
Customer due diligence related controls	Substantial
Risk understanding, assessment, and management	Substantial
Resources dedicated to AML/CFT and staff knowledge (including MLROs)	Moderate

10.2.7.4 Residual Risk

As indicated in the following residual risk table, the overall residual risk of laundering the proceeds of crime through high-value goods in Malta is 'medium-high', with the risk driven by the laundering of domestic proceeds from the acquisition of high-value motor vehicles, the acquisition of leisure yachts including concealment of BO and/or through chartering, and the concealment of ownership of motor vehicles including through hire purchase agreement or leasing. Here the mitigating measures in place are not effective and robust enough in order to address the inherent risk.

Table 82: Residual risk table – dealing in high-value goods

Topic	Inherent Risk	Effectiveness of mitigating measures	Residual risk	Overall residual risk level
Laundering of domestic proceeds from the acquisition of high-value motor vehicles, including through the use of cash and/or instalments	High	Moderate	High	**Overall residual risk = Medium-high**
Acquisition of leisure yachts including concealment of BO and/or through chartering	Medium-high	Moderate	Medium-high	
Concealment of ownership of motor vehicles[88]	Medium-high	Moderate	Medium-high	
Leisure yachts as part of VAT fraud	Medium-high	High	Medium	
Laundering through the precious metals & stones	Medium	Substantial	Medium	
Concealment of ownership of aircraft registered in Malta[89]	Medium	Moderate	Medium	
Laundering of foreign proceeds through the acquisition of high-value motor vehicles	Medium	Moderate	Medium	
Laundering through auctioneers and works of art	Medium	Substantial	Medium	

10.2.7.5 Recommendations

This section presents recommendations to guide subject persons when applying mitigating measures on a risk-based approach.

Ensure a comprehensive understanding of the obligations surrounding 'The Use of Cash (Restriction) Regulations' (S.L. 373.04) with a view to implementing the necessary measures and controls for the non-acceptance of cash exceeding the €10,000, and for the reporting of such attempts to the FIAU. Ensure that the €10,000 threshold is comprehensively monitored to cover linked transactions.

Monitor for any changes to 'The Use of Cash (Restriction) Regulations' (S.L. 373.04) as well as for any training and awareness on the legal obligations surrounding such legislation.

[88] Including through hire purchase agreement or leasing.
[89] Any concealment in relation to other legal persons refer to the other chapters.

10.3 Virtual Financial Assets and Virtual Financial Asset Service Providers

The VFA[90] sector in Malta consists of VFA Agents, VFA Services Providers and VFA Issuers. The VFA sector, which in November 2018 had 180 entities expressing interest, is smaller than originally anticipated due to the departure of numerous operators from Malta following the introduction of the regulatory regime and the operative provisions of the Virtual Financial Assets Act (Cap 590 of the Laws of Malta) in November 2018.

The Virtual Financial Assets Act[91] encompasses persons providing services in relation to virtual financial assets, including custodians, crypto asset exchanges (inclusive of fiat-to-VFA, VFA-to-VFA and VFA-to-fiat transactions), brokerage and portfolio management, as well as issuers of VFAs as part of an initial offering to the public, or the placing of such VFAs on trading platforms. The law also created the concept of a VFA Agent, who acts as an introducer to the virtual financial asset business into Malta. In 2022 Malta had 11 licensed VFASPs. Malta is not a market leader in terms of VFASPs on a global level, as the number of licenced VFASPs represents less than 0.5% of the global total reported population in 2021[92]. The vast majority of interactions by VFASPs licensed in Malta relate to an international clientele with less than 0.5% of clients that are resident in Malta. As at 31 December 2021 the total client base which is mostly retail, stood at just over six (6) million with approximately 56% of such clients being considered as active[93].

Subject persons are to assess their risks not only based on the analysis in their respective sectoral section, but also on additional sections, such as the overall ML risks 'section 11', 'section 12', that presents the TF risks, 'section 13' on PF and TFS related risks, as well as the other instruments as described in 'section 9'.

10.3.1 ML/TF/PF/TFS threats

In assessing the threats relating to the Virtual Financial Assets (VFAs) and the Virtual Financial Asset Service Providers (VFASPs) sector, the threats taken into consideration are in relation to:

- Licensed VFASPs in Malta
- Unlicensed VFASPs in Malta
- Laundering through crypto currencies (regardless of where there is a VFASP involved or its location) in Malta or by Maltese.

The vast majority of interactions by VFASPs licensed in Malta relate to an international clientele. As at 31 December 2021 the total client base which is mostly retail, stood at just over six (6) million with approximately 56% of such clients being considered as active (that is, clients who have carried out at least one transaction in the previous six-month period). This level of inactivity is not unsurprising in the crypto sector as many retail clients tend to invest a small amount of money in crypto assets and hold on to their investments without trading on a frequent basis. Moreover, 73.4% of the total client base are foreign and resident or otherwise incorporated or their

[90] In this iteration of the NRA, the term Virtual Financial Assets, which is the terminology used within the VFA Act, is being used interchangeably with crypto assets.
[91] https://legislation.mt/eli/cap/590/eng/pdf
[92] FATF (2021), Second 12-month Review Virtual Assets and VASPs, FATF, Paris, France
[93] Clients who have carried out at least one transaction in the previous six-month period

principal place of business is Europe excluding Malta, less than 0.5% of clients are locally resident in Malta and the remaining customers reside in non-EU/EEA jurisdictions. The strong international element in this sector is also evident from the number of requests, cases and suspicious reports handled by the FIAU and the MPF.

In 2021, a European Investigative Order was received by the Office of the AG that involved VFAs and it concerned the offences of hacking, unauthorised access, manipulation of computer data, swindling and money laundering. Investigations showed that the victim's ledger was hacked which led to various crypto currencies being stolen. Part of these crypto currencies were transferred to various exchanges, allegedly some were also transferred to a company registered in Malta.

The police-to-police requests received in 2021 reflected cases whereby the victims were Maltese and did not involve licensed VFASPs in Malta. In 2021, the MPF sent 55 requests for information to foreign countries of which more than half of the requests were sent with regards to one specific service provider only. Another five (5) European Investigative Orders were sent in relation to this one specific service provider in 2021 by the MPF.

There were a number of requests for information received by the FIAU from 19 different foreign counterparts related to cryptocurrency. The majority of these requests had the value ranging between €10,001 - €50,000, a small amount had the value ranging between €5 million to €10 million and one (1) being between €10 million to €50 million.

A small share of the suspicious reports received by the FIAU in 2021 submitted by different sectors other than VFAs, related to cryptocurrency and cryptocurrency wallets. Financial institutions in the form of payment service providers reported the highest number of STRs that related to cryptocurrency and cryptocurrency wallets followed by those offering electronic money and by credit institutions and remote gaming companies.

A relatively higher number of suspicious reports were submitted by the domestic VFASPs, where the top reasons for suspicion were due to the dark web (child pornography), the unknown source of wealth and source of funds and related to the subject or persons linked to the STR. Furthermore, a smaller percentage share of the STRs submitted by the VFASPs, was in relation to the suspicion of terrorist organisations that may be using different types of crypto assets for fund raising by advertising their wallet addresses on social media. The STRs submitted by VFASPs with terrorism related indicators all led to disseminations on TF suspicions to foreign FIUs. In addition, at par with the percentage share in relation to TF suspicions, were the STRs submitted by VFASPs due to the suspicion of there being the carrying out of a regulated activity but without an adequate license.

The number of financial crime investigations launched by the Blockchain Analysis Unit within the MPF in relation to crypto related cases, have more than doubled from 2020 to 2021. By 2021, around 25% of the financial crime investigations were in relation to crypto-related asset cases.

In 2021, the ARB was involved in four (4) cases out of 94 cases that had the freezing of the assets in 2021, where in these four (4) cases related to crypto assets, three (3) national, and one (1) foreign case, the ARB assisted the foreign counterparts in the freezing of crypto assets. In the foreign case,

the authorities had issued a freezing order in their country and requested the ARB to recognise and execute this freezing order in Malta as stipulated under EU Regulation 2018/1805 on the 22 April 2021. The same authorities informed the ARB that a subject person had gained possession of a monetary sum, through an aggravated means of payment fraud and changed them into bitcoins and subsequently transferred them to Malta. The ARB made several checks with different authorities and later informed the foreign counterparts that the ARB had recognised the freezing order on the same day. The ARB with the assistance of the FIAU and MPF, confirmed the location of the bitcoin and executed the foreign freezing order by executing it in Malta on the 23 April 2021. These crypto assets are still frozen.

Therefore, the above key findings indicate that the likelihood of abuse in relation to VFAs is relatively on the high side with indications of a higher abuse of the VFAs from the foreign market rather than the local VFASPs, as reflected in the following table:

Table 83: Rating of ML/TF/PF/TFS threats – VFAs and VFASPs

Threat	Impact	Likelihood	Threat level
Abuse of cryptocurrencies through the licensed VFASPs			
Domestic resident victims of crime involving crypto unrelated to domestic VFASPs (cybercrime, fraud)	Significant	Very likely	High
Circumvention of sanctions through crypto assets	Severe	Possible	Medium-high
Use of VFAs for TF purposes	Severe	Unlikely	Medium-high
Use of VFAs for ML purposes through licensed domestic VFASPs by foreign residents	Severe	Possible	Medium-high
Tax crime proceeds laundered through the use of cryptocurrencies	Significant	Possible	Medium
Use of VFAs for ML purposes through licensed domestic VFASPs by local residents	Significant	Unlikely	Medium
VFASPs being controlled by the criminal and their associates	Severe	Very unlikely	Medium
Abuse through the unlicensed VFASPs and laundering through VFAs in Malta			
Use of VFAs for ML purposes in Malta through foreign unlicensed VFASPs	Significant	Very likely	High
Use of VFAs for ML purposes through unlicensed domestic VFASPs by local residents	Significant	Unlikely	Medium

10.3.2 Vulnerabilities

This section presents the key findings of the analysis carried out on the vulnerabilities in this sector, where again by vulnerabilities here it is implied that these are weaknesses whose exploitation may allow threats to be translated into ML and TF. The key vulnerabilities identified are in relation to the level of activity, the non-face-to-face onboarding, the lack of education for the general public, the unregulated counterparts, and the ability to investigate crypto assets. The sector's exposure to the large volumes and nature of the business could in itself be considered a vulnerability. The VFA sector is the smallest in terms of the number of subject persons in Malta. However, the number of

transactions the sector generates is very large in comparison. During 2021 the Annual Transaction Value represents approximately 3% of the global trade. Local VFASPs serviced a total of six (6) million global customers which is also disproportionately large due to the size of the domestic market, with over 99% of the client base being foreign. While the majority of the clients are from an EU/EEA jurisdiction the remaining are spread across other jurisdictions.

Another key vulnerability is that in terms of the Maltese criminal law procedure all documents produced and exhibited as evidence need to be converted to a physical document, that is, to a written document. For example, if a laptop or a mobile is exhibited, an expert has to be nominated by the Court to extract the data and print the data to form part of the criminal court file. On the other hand, offences involving VFAs involve evidence that essentially is not paper based or is very difficult to reduce to paper evidence. Another problem that is encountered when dealing with virtual financial assets is the production of witnesses: given the cross-border element of these types of crimes, some of the evidence may be located in countries outside Malta. The method of obtaining evidence from abroad in the criminal justice sphere is through mutual legal assistance which requests may take long to be executed.

VFASPs lend themselves to be abused for ML due to the very nature of the product itself. VFSAPs allow transactions to take place anonymously, and the level of anonymity depends on the type of VFA. Technological means to further obfuscate the ownership of VFAs such as coin mixing and tumbling services further increase the risks of anonymity in this sector. The speed within which transactions take place and the irrelevance of one's physical location further increase the risks of the sector. Being an all on-line exclusive sector format, VFASPs can only onboard customers on a non-face-to-face basis. This increases the risk during the Know Your Customer (KYC) process as VFASPs may be dealing with a customer who is not who he/she says they are, increasing the risk of identity theft, forged documents being submitted, and other offences relating to misrepresentation.

Some customers may be uncooperative, refusing to provide sufficient source of wealth or source of funds information and documentation. In fact, unknown SoW/SoF or the client refusing to submit such information when asked by the VFASP accounted for 43% of the reasons why STRs were raised during 2021. Such clients generally opt to move to less regulated jurisdictions which intrinsically demand less stringent on-boarding processes. This thus leads to a high vulnerability in this sector.

Specialised roles, namely MLROs and Compliance Officers are in very short supply, and this results in the few available officials occupying multiple involvements with other subject persons, which may impinge on the effectiveness of the role because of lack of time commitment. This vulnerability is a common trend within the financial services in general in Malta and is one that indicates a skills shortage in AML/CFT. However, this is felt even more in the VFA sector as it is a very specialised sector and requires also a deeper understanding of the underlying blockchain technology. This vulnerability is further accentuated due to lack of available specialised AML/CFT training in this sector.

Table 84: Rating of the vulnerabilities – VFAs and VFASPs

Vulnerability	Impact	Exposure	Vulnerability level
Level of activity	Severe	High	High
Non-face-to-face onboarding	Significant	Very high	High
Lack of education for the general public	Significant	Very high	High
Unregulated counterparts	Severe	Very high	High
Ability to investigate crypto assets	Severe	High	High
Cross border transactions & exposure to HRJ	Significant	Moderate	Medium-high
Limited talent pool	Significant	High	Medium-high
Technology & outsourcing	Significant	High	Medium-high
Payment methods & anonymity	Significant	High	Medium-high
Maturity of the VFA sector	Significant	High	Medium-high
Legal gaps with regards to the taxation of crypto	Significant	High	Medium-high
Population of the VFASPs	Moderate	Moderate	Medium-low

10.3.3 Effectiveness of mitigating measures

A vital AML/CTF control which has been introduced to the VFA Framework is the role of the VFA Agent, which acts as a gatekeeper to the VFA Sector, ensuring that all prospective VFA license applicants are fit and proper, before they are onboarded with the VFA Agent, who will guide them through the application process. Additionally, when appointed in terms of Article 7 of the VFA Act (i.e., Issuers), the role of the VFA Agent is of a continuous nature, ensuring that issuers of VFAs remain fit and proper on an ongoing basis, until such time as the Initial VFA Offering (IVFAO) is concluded. Malta has also implemented an effective and robust regulatory regime through the VFA Act to regulate all VFA services offered from Malta. With this regulatory framework Malta has reduced significant AML/CFT risks related to VFA as all industry operators, including VFA issuers, VFASPs and VFA agents, are considered as subject persons under the PMLFTR, which offers a stronger approach than that which is taken across the rest of Europe with the implementation of the 5th Anti-Money Laundering Directive.

The standards imposed by the MFSA's regulatory regime for VFA service providers has proven to be effective in acting as a filter, ensuring that only serious market players with a strong compliance framework are present in Malta. This is evidenced by the number of applications submitted and the ones which were ultimately authorised.

Furthermore, the authorities, namely the MFSA and the FIAU, carried out over 50 supervisory interventions on the licensed VFASPs, in the form of onsite visits being either full-scope reviews or targeted examinations, *ad hoc* meetings, desk-based reviews, full-scope or targeted examinations. Sanctions were taken as a result of findings of such interventions, including sanctions taken by the MFSA[94] as well as enforcement action by the FIAU due to the breaches

[94] https://www.mfsa.mt/publication/okcoin-europe-ltd-the-company/
https://www.mfsa.mt/publication/moonpay-limited-the-company/
https://www.mfsa.mt/publication/moonpay-limited-the-company-2/
https://www.mfsa.mt/publication/nmva-ltd-the-company/

identified, whereby a total of €463,235 in pecuniary fines were imposed. However, given the appeals for some of these breaches, improvements are needed with regards to the level of effectiveness of final enforcement measures after appeal for breaches of AML/CFT obligations.

Furthermore, it is to be noted that in collaboration with the MBR, the MFSA has undertaken several initiatives to ensure that entities providing potential licensable activities without the necessary licence are prohibited from operating in or from Malta.

The VFA Framework also has inbuilt requirements that enhance the AML/CFT regime in Malta, such as the prohibition of services in relation to VFAs which have in-built anonymisation functions[95] unless the Licence Holder is able to identify the holder and transaction history of such VFAs. Furthermore, the PMLFTR requires VFASPs to identify the originator and beneficiaries of transactions. Due to the online nature of the sector, cash payments are not available. Since VFASPs rely substantially on technological platforms, and sometimes also use smart contracts, the VFA framework further obliges VFASPs to submit annual IT Systems audit reports which are done by independent third parties to the Authority. Such reports assess the robustness of the technological setup and thus give additional assurances that integrity exits in such a way that the technology cannot be used to facilitate illicit activities.

In order to mitigate the limited talent pool, MLROs being engaged by VFASPs undergo a rigid mandatory interview by FIAU officials in collaboration with MFSA, to ensure there is a high level of knowledge and understanding, not only in the subject matter including ML/TF, application of global sanctions, knowledge of anti-bribery and corruption and also anti-tax crime, but also related to the VFA sector ML/TF specific risks. Authorities also ensure that adequate time allocation is being observed, especially when multiple involvements with different regulated entities are present.

With regards to the extension of the Travel Rule by the FATF to the VFA space, such an introduction of such legal obligations will enhance the robustness of the AML/CTF regime once implemented as information on the originator and beneficiary will be available to competent authorities at all stages of the transfer process. However, it must be pointed out that full effectiveness will only be achieved once the Travel rule is applicable to all VFASPs in all jurisdictions, which will invariably take several years to achieve. Currently, local VFASPs are still obliged to obtain and store information of their customers, and therefore are only missing the obligation to transfer information to other VFASPs.

With regards to the subject persons themselves, some key findings are that 70% of VFASPs use partially automated transaction monitoring, while 30% are manual. 10% of VFASPs perform transaction monitoring in real-time, 40% as a post event process, and 50% as a combination of both. While the VFA Sector is the most recent sector that has been subjected to AML/CFT preventative measures, the number of reports submitted in 2021 was quite encouraging, as is their usability, especially when the quantity is compared to that of 2020. However, here it is to be noted that this reporting is not widespread across all the licensed VFASPs so there is an element of under-reporting by some VFASPs.

[95] R3-3.4.5.1 of Chapter 3 of the VFA Rulebook

The overall effectiveness of mitigating measures in this sector is that of 'substantial', where no improvements are needed with regards to licensing and authorisation process, minor improvements are required in the prudential supervision, the level of AML/CFT supervision and the guidance and outreach for the subject persons, moderate improvements are needed on the remediation, enforcement of administrative measures, as well as with regards to supervision of unlicensed activity. Improvements are needed in relation to public awareness, as well as the other factors that incorporate the travel rule, which as explained is applicable to all VFASPs in all jurisdictions.

With regards to the controls by the subject persons, moderate improvements are needed with regards to the risk understanding and risk assessment that will further enhance the quantity and quality of the STRs albeit it should be mentioned that the quality of the STRs that were received by the FIAU were of high quality in terms of their usability. However, VFAs that are under reporting will benefit from increasing their control levels as well as their risk understanding, and this will in turn lead to more and better quality STRs. Moderate improvements are also needed in terms of the AML/CFT governance, the resources dedicated to AML/CFT and staff knowledge, and the MLRO turnover rate.

Table 85: Effectiveness of mitigating measures – VFAs and VFASPs

Controls put in place by regulators	
Level of dissuasiveness of final enforcement measures after appeal for breaches of AML/CFT obligations, AML/CFT guidance and outreach, level of AML/CFT supervision, national cooperation between the authorities, fitness and proper checks.	High
Other factors (implementation of travel rule – domestically and foreign)[96] and public awareness	Moderate
AML/CFT controls by subject persons	
Reporting of STRs	Substantial
Customer due diligence related controls	Substantial
Risk understanding, assessment and management	Substantial
Resources dedicated to AML/CFT and staff knowledge (including MLROs)	Substantial

10.3.4 Residual risk analysis

As indicated in Table 86 the overall residual risk of the VFASPs sector is that of 'medium'. Further to this analysis, the overall residual risk of the sector is that of 'medium', which is taking into consideration the abuse through the licensed VFASPs and the abuse through the unlicensed VASPs. The overall residual risk is driven by the risk of abuse through the licensed VFASPs where there are domestic resident victims of crime involving for example cybercrime and fraud, as well as the tax crime proceeds that are laundered through the use of crypto currencies. Furthermore, there is as well the risk of abuse through the unlicensed VFASPs with the risk of abuse of cryptocurrencies for ML purposes in Malta through these foreign unlicensed VFASPs.

[96] This is a global issue and not only country specific.

Table 86: Residual risk table – VFAs and VFASPs

Topic	Inherent risk	Effectiveness of mitigating measures	Residual Risk	Overall residual risk level
Abuse of VFAs through the licensed VFASPs				
Domestic resident victims of crime involving crypto unrelated to domestic VFASPs (cybercrime, fraud)	High	Substantial	Medium-high	**Overall residual risk = Medium**
Tax crime proceeds laundered through the use of crypto currencies	Medium	Low	Medium-high	
Circumvention of sanctions through cryptocurrencies	Medium-high	High	Medium	
Use of cryptocurrencies for TF purposes	Medium-high	High	Medium	
Abuse of cryptocurrencies for ML purposes through licensed domestic VFASPs by foreign residents	Medium-high	High	Medium	
VFASPs being controlled by the criminal and their associates	Medium	Very high	Medium - Low	
Abuse of VFAs through the unlicensed VFASPs				
Abuse of cryptocurrencies for ML purposes in Malta through foreign unlicensed VFASPs	High	Substantial	Medium-high	
Abuse of cryptocurrencies for ML purposes through unlicensed domestic VFASPs by local residents	Medium	High	Medium-low	

10.3.5 Recommendations

This section presents a number of recommendations to guide subject persons when applying preventative measures on a risk-based approach.

Enhancing the risk-based approach

VFASPs should align the business risk assessment and the customer risk assessment with the results of the NRA and take steps to update the customer risk profiles as part of ongoing monitoring procedures, thereby ascertaining the risks identified are current. Furthermore, VFASPs should also review their CDD procedures, both at onboarding stage and as part of their ongoing monitoring obligations, to ascertain that these are risk-based, reflect the outcome of the NRA and are commensurate with the risks identified.

Monitor effectiveness of transaction monitoring systems for national and emerging risks
VFASPs should assess and monitor the effectiveness of their transaction monitoring system to ascertain that these allow proper detection of transactions that may be related to emerging risks, such as transactions relating to criminal proceeds, TF, fraud or cybercrime indicators, in line with the findings of the NRA. VFASPs should also ensure that assessment of the effectiveness of their transaction monitoring system also takes into consideration the submission of good quality and material STRs.

Improve the talent pool
VFASPs are to ensure an ongoing employee training programme which also includes basic and induction training on Crypto (types of wallets and DLTs in general), training of typologies (e.g., NFTs, and stablecoins) and trends, and possibly more technical on basic blockchain analysis.

Continue taking remedial action to address weaknesses in AML/CFT control framework
VFASPs should continue to take steps to assess the effectiveness of their AML/CFT control frameworks and take action to address any weaknesses identified, such as through the implementation of self-imposed remedial action plans and through cooperation with supervisory authorities to address any shortcomings identified during supervisory examinations.

11 Overall Money Laundering risk

11.1.1 Money laundering threats

This section presents an analysis of the money laundering threats occurring in Malta including the threats for laundering proceeds of both foreign and domestic proceeds of crime.

11.1.1.1 Threat of laundering of proceeds of domestic crime in Malta

The analysis of the 2023 NRA found that the following predicate offences are the main threats for laundering of proceeds of domestic crime in Malta:

Table 87: Rating of ML threats of domestic proceeds of the most significant crime

Drug trafficking	Medium-high
Organised crime	Medium-high
Fraud	Medium
Corruption	Medium
Tax crime	Medium

Table 88: Likelihood and the impact of the threats of ML of domestic proceeds of the most significant crime

Impact ►	Negligible	Minor	Moderate	Significant	Severe
Likelihood ▼					
Very Likely					
Likely			Tax crime, Fraud	Drug trafficking, Organised crime	
Possible			Corruption		
Unlikely					
Very Unlikely					

.

In the above risk matrix, drug trafficking and fraud are of a higher threat with regards to the laundering of the proceeds of domestic crime in Malta. Key findings are presented in the sections that follow on each main predicate offence.

11.1.1.1.1 Drug trafficking

Through the 2021 risk assessment of ML related to organized crime in Malta, the analysis carried out found that the size of the drugs market pertaining to organized crime groups in Malta in 2020 was estimated to be ranging from a low €51.8 million to a high of €86.3 million. In turn, STRs that had at least one Maltese resident involved, also featured drug trafficking or the illicit trafficking in narcotic drugs and psychotropic substances as a high attributable predicate offence. Drug trafficking was also the top predicate offence that led to the freezing of assets.

11.1.1.1.1 Organized crime

There are three types of organised crime in Malta. The first one is where you have the people in Malta as the victims, the second type is when you have the organised crime groups based overseas and use Malta to launder their proceeds including using Malta as a transit destination, and the third type is where the groups are based locally, and the laundering of the funds is done locally. Thus, the threat of ML stemming from organised crime can originate both from foreign and domestic offences, however this section deals with organised crime the perpetrator is based locally, and the proceeds of crime are laundered in Malta. It should be noted that in recent years there has been an increased influence of foreigners involved in the local organised crime scene especially in relation to narcotics. From the quantitative and anecdotal evidence provided, organised crime has a high likelihood to take place in Malta, however there is a lack of financial footprint in Malta and lack of visibility in view of the use of cash. In fact, local organised crime groups appear to have a limited financial footprint in Malta, and in most cases resort to untraceable means to launder their proceeds of crime such as through the use of cash. When addressing local ML, the local organised crime groups launder their proceeds either locally through real estate, cars, and investments or abroad usually through the same commodities. Local organised crime groups are found to be linked to predicate offences in relation to drug or human trafficking, counterfeiting activity, arson, theft, fraud and tax crimes (undeclared income).

11.1.1.1.2 Fraud

This was one of the main predicate offences in financial crime investigations, and also one of the highest attributable predicate offences in STRs involving a natural or legal person in Malta. The main typologies identified through such reports are:

- Increase in account turnover through cash and cheque deposits which are not in line with the customer's known profile
- Use of local owned legal persons
- Use of false documentation/forms
- Use of cash

With this type of predicate offence, it should be noted that the threat level is that of medium in view of the fact that the proceeds of crime are of a lower value than the other predicate offences, thus leading to a lower impact. There were only a few outliers during the period under review where the proceeds of crime were of a more significant amount.

11.1.1.1.3 Tax crime

Tax crime including domestic VAT fraud, is likely to take place in Malta however this predicate offence will have a lower value of proceeds of crime because of the lower nominal sums involved. This is especially so when one takes into consideration the fact that the majority of legal persons that defaulted in their submissions of tax and VAT returns were owned by Maltese shareholders/BO. Furthermore, with a significant use of cash and the size of the informal economy (estimated to range between 15.3%-23.6% of Maltese GDP)[97] there is a high likelihood of cases

[97] Central Bank of Malta (2020), An analysis of the shadow economy in Malta: A Currency Demand and MIMIC model approach - WP/02/2020.

of laundering of proceeds of this predicate offence in Malta, however the proceeds are of a lower value than for example under the laundering of foreign tax crime cases.

11.1.1.1.4 Corruption

Corruption is rated as 'medium' because although the predicate offence is likely to occur in Malta, the laundering of the proceeds of the crime is generally laundered outside Malta. In fact, the main typologies noted in cases or reports on corruption involving domestic residents mainly included foreign bank transfers, complex structures which usually involve multiple products and span over a number of jurisdictions. Under this predicate offence there were some significant outliers of proceeds of crime as well, albeit very few.

11.1.1.2 Threat of laundering of proceeds of foreign crime in Malta

The following predicate offences are the main threats for laundering of proceeds of foreign crime in Malta:

Table 89: Rating of threats of ML of foreign proceeds of the most significant crime

Organised crime	Medium-high
Tax crime	Medium-high
Fraud (incl. cybercrime)	Medium-high
Corruption	Medium
Drug trafficking	Medium

Table 90 presents the likelihood and the impact risk matrix for the main predicate offences of which the laundering of the proceeds of crime occurs in Malta.

Table 90: Likelihood and the impact of the threats of ML of foreign proceeds of the most significant crime

Impact ►	**Negligible**	**Minor**	**Moderate**	**Significant**	**Severe**
Likelihood ▼					
Very Likely			Fraud (incl. cybercrime)		
Likely				Organized crime	
Possible					Tax crime
Unlikely				Corruption Drug trafficking	
Very Unlikely					

11.1.1.2.1 Fraud (including cybercrime)

Fraud is the highest predicate offence on which assistance was sought in 2020 and 2021 from the OAG through the MLAs. Cybercrime also recorded a higher share of such offences in 2020 from the corresponding 2019 share, which is in line with the findings of the FATF's report on COVID-

19 ML trends[98], and also in line with the findings that are being presented in this document. Furthermore, apart from being one of the key attributable predicate offences in the reports received by the FIAU, when assessing the STRs reported with this predicate offence the indicative amounts involved were of a relatively high amount compared to the other top predicate offences reported. Fraud was also another key attributable predicate offence in the requests for information that were received by the FIAU in 2021. Specific typologies identified in these reports were forged documentation, use of complex corporate structures, transaction activity which is unexplained or not in line with customer/ business profile, and card fraud in the case of fraud related ML cases involving the use of remote gaming accounts.

11.1.1.2.2 Organized crime

Organized crime with an element of ML featured, albeit not ranking as the top category, in the incoming MLAs submitted to the OAG, although it is to be noted that there was a decrease from 2020 to 2021. In 2021, incoming MLAs with the predicate offence of organized crime and an element of ML stood at 3.3% of the total incoming MLAs from 4.8% in 2020.

In addition, investigations by the MPF also indicate organized crime in the form of smuggling of migrants to Malta and organized crime in the form of facilitating the movements of migrants by procuring documents to exit Malta, where the proceeds of crime in initiated investigations are estimated as much higher than the estimated value of proceeds in successful predicate offence investigations in view of the difficulty in detecting third parties as well as the fact that there is the use of cash that is untraceable. It is also to be noted, that in the 2021 risk assessment of ML related to organized crime in Malta and possible links between organized crime and terrorism, the main crimes identified in the 2021 organised crime risk assessment were considered to be (i) drug trafficking, (ii) human trafficking in terms of exploitation of low-paid labour and (iii) to a lesser extent smuggling of illicit goods.

There are various typologies in relation to this predicate offence, including:

- Misuse of Maltese Bank Accounts by Foreign Individuals linked to foreign OCGs
- Ownership of gaming companies / Credit and financial institutions by foreign OCGs (It is to be noted that since these cases were identified, the MGA and the MFSA have substantially revised and enhanced their licensing checks to avoid a reoccurrence of such cases.)
- Misuse of Maltese registered legal persons by foreign OCGs
- Setting up of Maltese registered legal persons despite having no additional nexus to Malta (no presence or operations in Malta, nor ownership by Maltese ultimate beneficial ownership).
- Maltese registered legal persons having shareholding held through other corporate vehicles with links at times to jurisdictions known for lack of beneficial ownership transparency.
- Local bank accounts of such companies do not present the expected economic activities of a trading company, with companies being usually used as money conduits.
- Complex transactions without apparent reasons undertaken through the bank accounts of such corporate vehicles.
- Financial statements for such corporate vehicles were not submitted regularly and/or not submitted.

[98] https://www.fatf-gafi.org/en/publications/Fatfgeneral/Updated-covid-19-ml-tf.html

- The use of loans to justify movement of funds was being noted. The terms of such loans (interest free, and no repayment date) indicate that such loans could be fictitious to cover up the movement of funds.

11.1.1.2.3 Tax crime

As indicated in the national risk assessment of tax offences and related ML, there is a significant inherent threat of ML in Malta derived from proceeds of tax crimes committed abroad occurring through for example the setting up of companies in Malta. However, it is noteworthy that in the incoming MLAs, tax crime does not account for the highest share of the incoming requests. The same applies to police-to-police requests and in the exchange of information requests received from the MTCA. However, the indicative amounts with regards to the incoming requests in relation to tax crime was quite substantial in comparison to the figures of other predicate offences in 2021. The use of cash-based businesses is also a common typology of cases relating to VAT fraud and tax crime. Key findings of the national tax risk assessment are available on the NCC website on the following link: https://www.ncc.gov.mt/wp-content/uploads/2023/03/Keyresults_taxriskassessment_final16122021-1.pdf

11.1.1.2.4 Drug trafficking

The laundering of proceeds in Malta of foreign drug trafficking is considered as 'medium' given that the drug scene locally has changed considerably over the past decade from a scenario were local drug dealers made individual arrangements on a one-to-one basis with foreign suppliers or even making personal arrangements to smuggle drugs into Malta, to a scenario where foreign organised crime groups are now providing the drugs to the local dealers. The *modus operandi* now is one where payments for the drugs are made in separate payments through the use of couriers who at times are also used to move the drugs themselves from one country to another. These couriers deliver the payments to the vendor's country of residence which in such cases is usually not Malta. The majority of seizures, that involve one kilogram of drugs or more, are normally all related to organised crime groups having a foreign component and therefore there is a significant amount of foreign proceeds of crime that is not being laundered in Malta.

11.1.1.2.4.1 Other predicate offences

If one were to assess the 'others' category of predicate offences, the top-ranking predicate offences excess currency/undeclared cash is one of the top-ranking predicate offences within this category with 5.4% of the total ML investigations. However, further to an analysis of the data, it follows that the ML threat of laundering foreign proceeds of crime in Malta via incoming cash declarations/undeclarations is low since the outgoing cash both declared and undeclared is always higher than that incoming. Nonetheless, the threat of laundering funds through such means still exists.

11.1.1.3 ML typologies

This section presents the salient typologies identified in main predicate offences.

11.1.1.3.1 Typologies of the laundering of proceeds of crime in Malta when there is at least one resident in Malta involved

Typologies identified in the laundering of proceeds of crime in Malta where there is at least one resident in Malta involved, are as follows:

Table 91: ML typologies

The use of cash and cash-based businesses
Abuse of complex corporate structures
Laundering through high value movables[99]
Comingling of funds between personal and business accounts
Structuring of cash deposits through various ATMs
Laundering through immovable property transactions
Misuse of locally owned companies

The use of cash, cash-based businesses, and the abuse of Maltese registered legal persons with no domestic activity are the key typologies in the ML threats identified in this section as further analysed in the working paper. The residual risk analysis of the typologies is presented in Table 97.

11.1.1.3.2 Typologies of the laundering of proceeds of crime in Malta when there is no domestic involvement

Typologies identified in the laundering of proceeds of crime in Malta where there is no domestic involvement, are as follows:

Table 92: ML typologies

Abuse of Maltese legal persons with no domestic activity
Trade based ML including transhipment activity
Abuse of legal persons and arrangements including through complex corporate structures
Abuse of Maltese registered legal persons as conduits in VAT fraud
Forged documentation
Laundering of proceeds through cross-border cash activity
Laundering of foreign proceeds of fraud through remote gaming operations
False Beneficial Ownership or concealment of Beneficial Ownership

The residual risk analysis of the typologies is presented in Table 97.

[99]

11.1.1.3.3 Other typologies

Apart from the typologies presented above, it is interesting to note the following additional typologies:

- Exploitation of low-paid labour
- Paying and receiving money solely through Escrow accounts (which is difficult to trace).

11.1.1 Vulnerabilities

This section presents the rating of the vulnerabilities, which focus on the overall AML/CFT/CPF TFS framework (for detailed analysis see sectoral sections).

Table 93: Ratings for the vulnerabilities

Vulnerability in the constitutional framework in the judicial review of sanctions that may impede or undermine supervisors from imposing proportionate, effective, and dissuasive administrative sanctions, including pecuniary penalties.[100]	High
Challenges in monitoring activities of legal persons with no links to Malta[101]	High
De-risking[102]	High
Limited pool of professional human resources	High
Vulnerabilities in the judicial system including the committal proceedings[103], the ML trial without jury, and the virtual evidence and vulnerabilities in relation to selling of assets by the ARB during criminal proceedings	High
Lack of criminal defence regime protecting subject persons when submitting suspicious reports and there is the appropriate consent from the FIAU	Medium-high
Possible differences between sectoral MLRO approval procedures	Medium-high
Recognition framework for foreign gaming license holders[104]	Medium-high
Obstacles to authorities' cooperating and coordination in enforcement matters	Medium-high
Lack of sufficient and comprehensive criteria for quality of STR reporting	Medium
Vulnerability in fighting tax crime and the collection of taxes	Medium
Short-term of FIAU postponement order[105]	Medium
Harmonised statistics	Medium

[100] Refer to the Banking section on the 'effectiveness of the mitigating measures' sub-section 10.1.1.3.
[101] Refer to the Legal persons vulnerabilities sub-section 9.1.2.
[102] Refer to the VOs (NPOs) vulnerabilities sub-section 9.4.2, and the ML threats sub-section 10.1.1.1 of the Banking sector.
[103] Public Consultation - Reform for the Compilation of Evidence and Referrals Procedure - ġustizzja (gov.mt)
[104] Refer to the Gaming ML threats sub-section 10.2.1.3.2.
[105] Layout 1 (fiaumalta.org) p. 218

Table 94: Risk matrix for the vulnerabilities

Impact ►	Negligible	Minor	Moderate	Significant	Severe
Exposure ▼					
Very High				De-risking; Limited pool of professional human resources; Judiciary system including the committal proceedings, the ML trial without jury, and the virtual evidence and selling of assets by the ARB during criminal proceedings	Constitutional framework in the judicial review of sanctions
High				Lack of criminal defense regime protecting subject persons when submitting suspicious reports and there is the appropriate consent from the FIAU; Lack of comprehensive cross-sector approval procedures of MLROs; Recognition framework for foreign gaming license holders; Suspension withdrawal of licensing	Vulnerability in the administrative sanctions imposed by regulatory authorities; Challenges in monitoring threats in legal entities with no links to Malta
Moderate			Harmonized statistics; Lack of sufficient and comprehensive criteria for quality of reporting of STRs		
Moderately Low				Vulnerability in fighting tax crime and the collection of taxes Short-term of FIAU postponement order	
Low					

11.1.2 Money Laundering mitigating measures

By taking into account all the sectoral working groups, the following ratings are achieved in order to determine the effectiveness of mitigating measures:

Table 95: Effectiveness of mitigating measures in the sectoral working groups

Recognition notice framework	Moderate
Tax advisors	Moderate
Lawyers	Substantial
CSPs	Substantial
Financial Institution	Substantial
Investment services	Substantial
Dealing in high value goods	Substantial
Pensions	Substantial
Dealing in immovable property	Substantial
Lawyers	Substantial
Insurance	High
Remote gaming	High
Land-based gaming	High
Banking	High
Accountants and auditors	High
VFASPs	High

11.1.3 Money Laundering residual risk

Table 96 presents the residual risk rating of the laundering of the proceeds of crime happening in Malta and by predicate offence.

Table 96: Residual risk – laundering of the proceeds of crime by predicate offence

Topic	Inherent risk	Effectiveness of mitigating measure	Residual risk level
Laundering of proceeds in Malta from domestic drug trafficking	Medium-high	Substantial	Medium-high
Laundering of proceeds in Malta from local organized crime	Medium-high	Substantial	Medium-high
Laundering of proceeds in Malta from foreign organised crime	Medium-high	Substantial	Medium-high
Laundering of proceeds in Malta from foreign crime: fraud (including cybercrime)	Medium-high	Substantial	Medium-high
Laundering of proceeds in Malta from corruption in Malta	Medium	High	Medium-low
Laundering of proceeds in Malta from domestic tax crime	Medium	High	Medium-low
Laundering of proceeds in Malta from foreign tax crime	Medium-high	High	Medium
Laundering of proceeds in Malta from foreign crime: corruption	Medium	Substantial	Medium
Laundering of proceeds in Malta from foreign crime: drug trafficking	Medium	Substantial	Medium
Laundering of proceeds in Malta from domestic fraud	Medium	Substantial	Medium

The following table presents the residual risk ratings by typology:

Table 97: ML residual risk ratings by typology

Topic	Inherent risk	Effectiveness of mitigating measure	Residual risk level
Abuse of Maltese registered legal persons with no sufficient links to Malta, for ML or concealment of BO	High	Substantial	Medium-high
The use of cash and cash-based businesses	High	Substantial	Medium-high
Trade based ML abusing geographical location and transhipment activity	Medium-high	Substantial	Medium-high
Abuse of complex corporate structures for ML or concealment of BO	Medium high	Substantial	Medium-high
Laundering through high-value movables[106]	Medium-high	Substantial	Medium-high
Laundering through immovable property transactions	Medium-high	Substantial	Medium-high
Abuse of Maltese registered legal persons as conduits in VAT fraud	Medium-high	High	Medium
Cross border cash activity	Medium	Substantial	Medium
Laundering of foreign proceeds of fraud through remote gaming operations	Medium	Substantial	Medium

[106] Including through hire purchase agreement or leasing.

12 Terrorist Financing

In carrying out this risk assessment, the methodology adopted was that of the FATF guidance on the TF risk assessment[107], along with building on the risk assessment on TF that was carried out by Malta in 2019. It is to be noted that for the purposes of the TF risk assessment, the list of countries that fall under the category of high-risk jurisdictions was determined further to a thorough research aimed at identifying the jurisdictions considered to be either:
- state sponsors of terrorism
- the jurisdictions where terrorist groups are based or
- are known to be particularly active or in areas of conflict
- jurisdictions adjunct to the above

12.1 Threat of Terrorist Financing

TF involves the threat that funds or other assets intended for terrorists or terrorist organisations are being raised, moved, stored or used in or through a jurisdiction, in the form of legitimate or illegitimate funds or other assets. This section presents the ratings of the threat assessment of TF being raised, moved or stored in Malta, where the highest threats prior to assessing controls were found to be the threat of movement of funds through the involvement of Maltese registered legal persons in TF with no transfers through Malta, and the movement of funds for TF via financial institutions.

An analysis was carried out on the net banking flows sent to foreign jurisdictions from Malta in comparison with the remittance data and the trade data. The purpose of this analysis was to identify countries towards which either bank flows or outgoing remittances are identified despite these being countries with whom Malta has no trade activity. The analysis focused on 'outliers', namely countries that feature in the high-risk jurisdictions for TF purposes. The analysis showed that while in 2019 and 2020, there were 14 and 15 such countries respectively, the number reduced to seven (7) such countries in 2021, most of which forming part of Central, West or East Africa. All seven (7) countries identified in 2021, had featured in previous years. Another key conclusion here is that higher riskier countries are featuring under the financial remittances rather than bank flows. In the analysis on the outgoing remittances, the number of persons residing in Malta who are nationals of such countries was also taken into consideration, using as a source of data Identity Malta.

This section seeks to determine, the threat associated with raising and movement of TF funds through voluntary organisations (VOs) or non-profit organisations (NPOs) to high-risk jurisdictions. It is to be noted that as indicated in the VOs' (NPOs') section, 55 Maltese registered VOs (NPOs) fall within the FATF scope[108]. In addition, further analysis indicates that out of these 55, there are ten (10) VOs (NPOs) that generate revenue and income exceeding €250,000 annually. Furthermore, it is to be noted that the disbursements by VOs (NPOs) to the TF high-risk

[107] FATF (2019), Terrorist Financing Risk Assessment Guidance, FATF, Paris, Terrorist-Financing-Risk-Assessment-Guidance.pdf (fatf-gafi.org)
[108] 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".

jurisdictions in 2021 were carried out through credit institutions, bank transfers, cheques and card payments. No disbursements were done via financial remitters. The specific VOs (NPOs) also involved a subject person within their set-up.

In relation to the TF threat within the VFAs sector, especially when one considers that the VFASPs sector is one of the top reporting sectors (as addressed in section 10.3 on VFASPs in this document), the FIAU received a relatively low number of reports containing terrorism or TF related indicators. A report led to a dissemination to the MPF and a foreign FIU, while the remaining reports were disseminated to foreign FIUs. The other significant share of the reports was submitted mainly by the credit institutions, which were the top submitters, and by the remote gaming operators.

With regards to the threat of movement of funds via legal persons registered in Malta with a UBO from jurisdictions with active terrorist organisations and/or conflict zones, out of the legal persons registered in Malta in 2021 having a foreign BO, 7.6% have a BO that is a national of a high-risk jurisdiction from a TF perspective.

Another possible threat is in relation to the movement of funds through the beneficiaries of the trusts. From the data extracted from TUBOR, it results that these comprise of 1,342 Maltese beneficiaries reported, of which 1,243[109] are individual beneficiaries indicated as having Maltese nationality and 99[110] of which are legal persons' beneficiaries with Malta reported as being the country of registration. With respect to non-Maltese beneficiaries, it was noted that there are 5,098 beneficiaries reported, of which 421 emanate from high-risk jurisdictions. From these 421 (8.6%) beneficiaries, 406[111] are individual beneficiaries whose nationality is that of a high-risk jurisdiction[112] and 15[113] are legal persons' beneficiaries[114] which were registered in high-risk jurisdictions. In addition, with regards to trustees, the vast majority of the trustees who reported trusts on TUBOR are Maltese trustees. There are however 53 non-Maltese trustees who have also reported trusts on TUBOR, either as co-trustees to Maltese trustees or else as non-EU resident trustees establishing a business relationship in Malta. Out of these non-Maltese trustees reported on TUBOR, only one trustee is established in a high-risk jurisdiction, where the beneficiaries consist in a class, but the trust also has two protectors indicated as being nationals of another non-high-risk jurisdiction in terms of TF. From the total number of trusts whose beneficiaries are Maltese, there are no trustees from high-risk

[109] It should be noted that from the 1,243 individual beneficiaries with Maltese nationality, there are 255 from the reported beneficiaries which feature as beneficiaries in multiple trusts.
[110] It should be noted that from the 99 body corporate beneficiaries indicated as being registered in Malta, there are 38 of such reported body corporate beneficiaries which were feature as beneficiaries in multiple trusts.
[111] It should be noted that from the 406 individual beneficiaries identified whose nationality is from high risk jurisdictions, there are 60 from the reported beneficiaries which featured in multiple trusts.
[112] Some of the beneficiaries were reported on TUBOR as having dual nationalities. For the purpose of this exercise if a high-risk jurisdiction was included as one of those nationalities we included this under the total amount of individual beneficiaries whose nationality is that of a high-risk jurisdiction.
[113] It should be noted that from the 15 body corporate beneficiaries registered in high risk jurisdictions, there is one (1) reported beneficiary which was features in a two trusts .
[114] It should be noted that there are also four (4) body corporate beneficiaries which were registered in Kenya however for the purpose of this exercise for the reasons set out above, as this information was excluded since they were reported in relation to retirement schemes which were set up as trusts.

jurisdictions, which therefore, indicates that the threat of movement of funds via the beneficiaries is rather limited.

Another inherent threat for TF is in relation to the threat of abuse of Malta's geographical location as a transhipment hub. Malta's geographical position at the centre of a major trading route, close proximity to sanctioned countries as well as its Freeport, renders it susceptible to these kinds of intercepted cargo.

Furthermore, another key finding is that in 2020 there were no incoming international requests in relation to TF, and in 2021 there were only two (2) requests that were in relation to TF and these were sent by EU countries. The execution of the two (2) MLAs was effected. There were no outgoing international requests. On the incoming requests police to police cooperation that where on TF, the MPF received nil requests in 2020 and six (6) in 2021. With regards to requests in relation to terrorism, the majority of the international requests in relation to terrorism had no terrorism related suspicion after being addressed by the MPF. With regards to FIU to FIAU incoming requests, 20 requests were received over an 18-month period, however a large portion of these had no links to Malta and were blanket requests which were sent to all Egmont members following terror attacks which had taken place.

Therefore, in view of these key findings, the rating of the TF threats is as follows:

Table 98: Rating of TF threats

Threat	Impact	Likelihood	Threat level
Involvement of Maltese legal persons in TF with no transfers through Malta[115]	Severe	Possible	High
Movement of funds for TF via financial institutions	Severe	Likely	High
Movement of funds for TF via cash cross-border movements	Severe	Possible	Medium-high
Movement of funds for TF via credit institutions	Severe	Unlikely	Medium-high
Raising/Movement of funds for TF via disbursements of VOs (NPOs)	Severe	Unlikely	Medium-high
Trade-based TF	Severe	Possible	Medium-high
Raising/Movement of funds for TF via cryptocurrencies	Severe	Possible	Medium-high
Raising/movement of funds for TF via remote gaming	Severe	Possible	Medium-high
Movement of funds through beneficiaries of Trusts	Severe	Very unlikely	Medium
Involvement of BO in TF with no transfers through Malta	Severe	Very unlikely	Medium
Using TF funds domestically	Severe	Very unlikely	Medium

[115] This threat takes into consideration the findings on other international financial centres.

12.2 Vulnerabilities

This section presents the findings of the assessment of vulnerabilities that took into consideration:

- The finding that the financial remittance sector is more likely to be used than the banking sector and is therefore more likely to be exploited for illicit purposes.
- The fact that there are legal persons that do not bank in Malta, since data from the CBAR indicates that only 22% of the legal persons having the BO who is national from a TF high risk jurisdiction have a Maltese IBAN.
- Legal persons that are not submitting financial statements, since data from the MBR indicates that 23% of the legal persons that have the beneficial owner who is national from a TF high risk jurisdiction, did not submit a financial statement.
- The limitations in international cooperation due to the lack of adequate and/or timely responses to some requests that were made by Maltese authorities to foreign counterparts.
- Inability by the Customs Department (MTCA) to monitor the final destination of cash.
- TF risk understanding by voluntary organisations.
- Level of awareness of TF among the private and public sector, and ability to detect suspicious behaviour.

This leads to the following risk matrix, where the highest ranking is attributable to the vulnerability in view of lack of TF understanding of risk by financial remitters, and the less effective controls in the financial remittance sector:

Table 99: Rating of TF vulnerabilities

Vulnerability	Impact	Likelihood	Vulnerability level
TF lack of understanding of risk by financial remitters	Severe	High	High
Less effective controls in the financial remittance sector	Severe	High	High
Inability to monitor the final destination of cash	Severe	Moderate	Medium-high
Legal persons linked to HRJ which do not bank in Malta	Severe	Moderate	Medium-high
Legal persons linked to HRJ that are not submitting financial statements	Severe	Moderate	Medium-high
Lack of cooperation with countries at a higher risk of terrorism / TF	Severe	Moderate	Medium-high
VOs (NPOs) that fall under the FATF scope level of TF risk awareness	Severe	Moderate	Medium-high
TF lack of understanding of risk by credit institutions	Severe	Low	Medium

12.3 Effectiveness of mitigating measures

During the past years, the competent and law enforcement authorities have taken several actions in order to make sure that there is nothing left unaddressed and to ensure that Malta is assessing the risks of terrorism and TF from every possible angle. With regards to guidance and outreach, the FIAU issued guidance documents on TF, held webinars and outreach sessions, carried out strategic analysis on cross-border cash declarations and other relevant topics, carried out thematic supervisory reviews, and implemented enhancements to the FIAU's prioritisation and analytical process to improve the handling of TF cases.

The Customs Department (MTCA) enhanced their resources given the amendment in article 70C of the Customs Ordinance (CAP. 37) that enables the Commissioner for Tax and Customs to request information on all related Customs aspects emanating from border controls, thus necessitating enhanced resources. Furthermore, there was the amendment in the Cash Control Regulations, Subsidiary Legislation 233.07 that enables the Commissioner for Tax and Customs to detain any cash, whatever its value, whether it is being carried or unaccompanied, and whether it has been declared or not, where there are indications that the cash is related to criminal activity. Furthermore, as required under the Cash Control Regulations, any person entering or leaving Malta, or transiting through Malta and carrying a sum equivalent to €10,000 or more in cash (or its equivalent in other currencies) is obliged to declare such sum to the Commissioner for Tax and Customs, in an applicable Cash Declaration Form, where these declarations are received by the Department of Customs (MTCA). It is to be noted that for example, the FIAU also uses data obtained through cross-border cash declarations for its operational cases, whereby persons subject to suspicious reports are checked against the cash declarations data amongst other databases.

National cooperation was enhanced between the supervisory authorities and the law enforcement agencies with the use of task forces for example. In addition, a task force was set up between the SMB and the credit institutions to formalise a channel of communication whereby financial institutions, the SMB and law enforcement may exchange and analyse information as well as intelligence in a quick manner to detect, prevent or disrupt violations of sanctions and in particular instances consider the wider economic ML, TF and PF threats posed to the Maltese islands.

The OCVO holds periodic one-to-one meetings with the VOs (NPOs) which fall within the FATF Scope, with the aim of providing them with the relevant information on the risks there are and how to mitigate them. During the meetings, the OCVO highlights the continued importance to use bank transfers and authorised financial institutions where possible.

The following risk matrix shows the ratings on the assessment of the effectiveness of mitigating measures in place, where moderate improvements are needed in relation to the reporting of the TF-related STRs, particularly by financial remitters and the resulting quality of the STRs given the analysis of the financial flows that was carried out for this specific risk assessment.

Table 100: Rating of the effectiveness of mitigating measures - TF

Controls put in place by regulators	
Level of dissuasiveness of final enforcement measures after appeal for breaches of CFT obligations, CFT guidance and outreach, level of CFT supervision, national cooperation between the authorities, fitness and proper checks.	High
AML/CFT controls by subject persons	
Reporting of STRs	Substantial
Customer due diligence related controls	Substantial
Risk understanding, assessment, and management	Substantial
Resources dedicated to CFT and staff knowledge (including MLROs)	Substantial

12.4 Residual Risk

Based on the analysis of the threats and vulnerabilities that lead to the inherent risk, and the analysis of the control measures, the overall residual risk of TF being raised, moved, or used in Malta is 'medium'. This rating is mainly driven by the movement of funds for TF via financial institutions (remitters), the involvement of Maltese legal persons with BOs in high-risk jurisdictions possibly linked to TF (with no business relationship with the financial sector in Malta), and the threat of the movement of funds for TF via cash cross-border movements and the threat of raising/movement of funds for TF via disbursements of VOs (NPOs) that fall under the FATF scope where it is to be highlighted that only around 3% (55 out of 1,708) of the enrolled VOs (NPOs) with the OCVO are considered as falling under the scope of FATF recommendation 8.

Table 101: TF residual risk analysis

Topic	Inherent risk	Effectiveness of mitigating measure	Residual risk	Overall residual risk level
Movement of funds for TF via financial institutions (remitters)	High	Substantial	Medium-high	**TF residual risk = 'Medium'**
Involvement of Maltese registered legal persons with BOs in HRJ possibly linked to TF (with no business relationship with the financial sector in Malta)	High	Substantial	Medium-high	
Movement of funds for TF via cash cross-border movements	Medium-high	Substantial	Medium-high	
Raising/Movement of funds for TF via disbursements of VOs (NPOs) that fall under the FATF scope	Medium-high	Substantial	Medium-high	
Movement of funds for TF via credit institutions	Medium-high	High	Medium	
Movement of funds for TF via cryptocurrencies*	Medium-high	High	Medium	
Movement of funds for TF via remote gaming	Medium-high	High	Medium	
Trade-based TF	Medium-high	High	Medium	
Movement of funds through beneficiaries of Trusts	Medium	High	Medium-low	
Domestic raising of funds for TF	Medium	High	Medium-low	
Threat of abuse for TF by VOs (NPOs) that do not fall under the FATF scope	Medium-low	High	Medium-low	
Using TF funds domestically	Medium	Very high	Medium-low	

** This refers to the licensed VFASPs. For a full analysis on the crypto assets refer to section 10.3, where the analysis takes into consideration the licensed VFASPs in Malta, the unlicensed VFASPs in Malta, and the laundering through VFAs crypto currencies (regardless of where there is a VASP involved or its location) in Malta or by Maltese.*

12.5 Recommendations

This section presents a number of recommendations to guide subject persons when applying preventative measures on a risk-based approach.

Update the TF risk understanding in the risk assessment and risk management strategies.

Ensure alignment between policies, controls and procedures and the findings of the TF risk assessment.

Monitor the implementation of the updated controls and enhance them, if necessary.
Continue monitoring TF sanctions updates, and news items relating to countries of concern.

Ensure alignment between CDD obligations and transaction monitoring, in line with the findings of the NRA.

13 Proliferation Financing and Targeted Financial Sanctions related risks

This section presents the results of the risk assessment on PF and TFS related risks, with the objective of assisting the supervisory and law enforcement authorities and the private sector to identify, assess, understand, and mitigate Malta's PF and TFS related risks. In line with FATF Recommendation 1 and its Interpretative Note, the said risk assessment assessed Malta's risk with regards to the potential breach, non-implementation or evasion of targeted financial sanctions, and assessed as well as the broader risk of proliferation financing.[116]

The analysis of this risk assessment takes into consideration the Royal United Services Institute (RUSI) guide on conducting a PF risk assessment.[117]

Most of the data in this section is up to 2021. An updated threat and vulnerability analysis is therefore a high priority.

13.1 PF and TFS threats

Malta has to date had no specific cases evidencing proliferation financing, but Malta has withheld goods in transhipment, potentially connected to proliferation. Malta acknowledges however that it has a number of specific threats and vulnerabilities which could potentially be exploited by proliferation countries in the field of PF and enabling the raising and moving of funds specifically the moving of funds. In order to assess this, the following key findings are to be noted.

Two (2) of the main countries presenting PF risks are the DPRK and Iran. It is to be noted that no single permits and residence permits have been issued to nationals of countries of proliferation concern, it is to be noted that there were nil single permits and resident permits issued to nationals of DPRK, while only a very small number were issued to Iranian nationals.

Malta is also home to a foreign workers community, some of whom may originate from sanctioned countries. When considering the totality of foreign workers that are nationals of said countries, it results that the highest number originate from Serbia (42%), followed by Turkey (12%), Libya (7%), Ukraine (6%) and Russia (5%). On the other hand, out of the legal persons registered in Malta in 2021 with a foreign BO, 7% have a BO hailing from sanctioned countries in 2021. However, there are no known cases of Maltese registered legal persons being involved in proliferation financing. Furthermore, there are no active bank accounts belonging to DPRK nationals and a limited number of accounts belonging to Iranian nationals. No remittances have been effected to or received from DPRK in the period 2015-2022.

The threat arising from Malta's proximity to sanctioned countries coupled with Malta being a transhipment hub exacerbates Malta's risk for illicit traffic in goods for PF that would be

[116] https://www.fatf-gafi.org/en/publications/Financingofproliferation/Proliferation-financing-risk-assessment-mitigation.html. In line with footnote 7 of this document, the broader PF risks, which are not covered in the updated Recommendation 1, refer to the risk of weapons of mass destruction proliferation and the risk of financing of proliferation.

[117] Guide to Conducting a National Proliferation Financing Risk Assessment | Royal United Services Institute (rusi.org)

transported with regular shipping companies, notwithstanding the screening measures adopted by Customs' officers.

There is also a significant flow of goods through the Malta Freeport Terminal which processes three (3) million TEUs (twenty-foot equivalent units) containers per year over the period of 2019 to 2021. This increases the possibility that sanctioned goods are possibly shipped through the Malta Freeport Termina. When analysing the share of containers originating from the EU as against the share of those originating from non-EU countries in both the loading and the discharging in Malta, the share of the containers originating from non-EU countries is higher than that from the EU. However, it is to be noted that that the containers loading in Malta and originating from EU countries registered an increase from 2020 to 2021 while those from non-EU countries registered a decline. The same pattern was noted with regards to the discharging containers but in this area the decrease is less steep. Additionally, the ports of call from Malta Freeport Terminal are those in the Mediterranean.

Over the period of 2018 to 2021, there were over one thousand cases scrutinised by the Customs Department (MTCA). Out of these, only 5.5% were military/dual use goods, but ultimately did not result in any cases of PF.

In the cases analysed further by the STSMU where commercial invoices and documentation was requested and scrutinised, no cases involving Maltese financial institutions have been encountered. The STSMU performs background checks and assessment of exporter and consignee against listed entities and individuals against the periodically updated Financial Sanction Files, other intelligence derived listings and open-source online searches. Should a potential listed person/entity be identified, the matter would be referred to the SMB and an opinion is solicited. Since 2019, two (2) such cases have been referred, albeit with negative results. It is to be noted that exports to high-risk jurisdictions are controlled 100%, so for example, in 2019 there were zero (0) exports to Afghanistan, in 2020 there was one (1) export, and it was controlled, and same for 2021.

The use of cash couriers is another threat in relation to the raising and moving of funds without traceability. The large amount of cash that is being declared at the border, specifically the fact that the outgoing (€75 million) is much higher than the incoming (€27.7 million) over the period of 2017 to 2021, implies that there is a potential threat. In addition, the amount of assets restrained between 2017 to 2021 amounted to €3 million, where in some of the cases the nationals were hailing from high-risk jurisdictions.

While Malta does not manufacture military items, there are however there a small number of arms traders engaging in imports and exports of arms. Most exports of arms and military items consist in small arms intended for anti-piracy operations, one-off exports of sporting rifles/weapons intended for personal use, and repaired engines of military aircraft. The number of exports is limited, and there is no evidence that the arms trade in Malta is being abused for proliferation purposes.

Malta like any other jurisdiction, is exposed to cyberattacks, an area of concern when it comes to PF[118]. According to the NCSI[119], Malta has the lowest national cybersecurity index score in all of the EU, which includes in the composition of the rating the proliferation of spoofing, online shopping frauds and other types of attacks. Over the past three years Malta's Police Cybercrime Unit reported that the number of cybercrime investigations opened throughout the past three years were quite significant even though no incidence was connected to PF.

On the reporting of suspicious reports to the FIAU, in 2021 a total of 64 reports from subject reports and a handful from other international counterparts and other domestic authorities were sent to the FIAU, where these reports were connected to TFS and PF, including dual-use goods.

52% of the incoming reports were disseminated to SMB, where the majority of these reports were submitted by VFASPs and the remaining by two (2) domestic competent authorities.

Further to these key findings, the following table presents the rating of the threat of financial products and services directly related to trade in proliferation-sensitive goods, and the threat of licit and illicit revenue-raising activities.

Table 102: Rating of PF and TFS related threats

Threat	Impact	Likelihood	Threat level
Financial products and services directly related to trade in proliferation-sensitive goods			
Money transfer services used to conduct transfers related to procurement of goods	Severe	Possible	Medium-high
Use of trade finance products and services in procurement of proliferation-sensitive goods	Severe	Unlikely	Medium-high
Use of vessels and/or shipping companies and/or the aviation industry in the movement of sensitive goods and/or to evade sanctions	Severe	Possible	Medium-high
Use of personal accounts to purchase industrial items	Severe	Unlikely	Medium-high
Use of front companies with opaque ownership structures to obtain trade finance products and services as parties to clean payments	Severe	Possible	Medium-high
Use of legal persons registered in Malta with the BO hailing from sanctioned countries to mask parties to transactions and end users	Severe	Unlikely	Medium-high
Nationals or dual citizens of proliferating states, or family members of such persons (regardless of citizenship), used as intermediaries in Malta to facilitate the procurement of goods and/or for payment of funds.	Severe	Unlikely	Medium-high
Circumvention of sanctions through VFAs*	Severe	Possible	Medium-high

[118] As indicated in the FATF guidance document on PF, UNSCR 1718 PoE Report identifies that the DPRK had been using cyberattacks to illegally force the transfer of funds from financial institutions and VASPs (exchanges), as a means to evade financial sanctions and to gain foreign currency. Such attacks have become an important tool in the evasion of sanctions and have grown in sophistication and scale since 2016.

[119] NCSI: Malta (ega.ee)

Use of shell companies with the BO hailing from sanctioned countries, to obtain trade finance products and services as parties to clean payments	Severe	Very unlikely	Medium
Licit and illicit revenue-raising activities			
Cross-border smuggling of cash to support proliferation activities	Severe	Possible	Medium-high
Payments made to labourers or workers (nationals or dual citizens) from Iran, North Korea or other sanctioned countries, where these payments are then part of Iran or North Korea's or other sanctioned country revenue-raising activities	Severe	Possible	Medium-high
Illicit Arms Trading	Severe	Very unlikely	Medium
Construction industry and/or related trades owned or operated by or on behalf of nationals or dual citizens of North Korea or North Korean entities	Severe	Very unlikely	Medium
Sale of minerals (gold, iron, steel, copper, and zinc) by North Korea or involving North Korean designated entities and individuals to raise revenue	Severe	Very unlikely	Medium
Payments made to labourers or workers (nationals or dual citizens) from North Korea, where these payments are then part of North Korea's revenue-raising activities	Severe	Very unlikely	Medium
Exports originating from North Korea or involving North Korean designated entities and individuals	Severe	Very unlikely	Medium
Use of legal persons to conceal BO related to TFS	Severe	Very unlikely	Medium

**For a full analysis on the crypto assets refer to section 10.3, where the analysis takes into consideration the licensed VFASPs in Malta, the unlicensed VFASPs in Malta, and the laundering through VFAs crypto currencies (regardless of where there is a VASP involved or its location) in Malta or by Maltese.*

13.2 Vulnerabilities

The following table presents the rating of the vulnerabilities which refer to matters that can be exploited by the threat or that may support or facilitate the breach, non-implementation or evasion of PF TFS. The main vulnerabilities are Malta's proximity to sanctioned countries coupled with Malta being a transhipment hub, and the lack of sufficient knowledge or expertise by the subject persons. Whilst awareness on the obligations to adhere to international sanctions is increasing across the jurisdiction, there are still segments of the business sector who do not fully understand their obligations vis a vis sanctions. In principle this refers to the businesses which are not subject persons and have no legal obligations to have systems in place for the implementation of TFS in accordance with article 17(6) of the National Interest (Enabling Powers) Act. Meanwhile, with regard to PF, there is general lack of knowledge among private sector operators on the typologies concerning PF. This is coupled by a lack of sufficient knowledge on items which can have dual use purposes and their possible use for proliferation and their procurement through the services of intermediaries.

In addition, there is also the vulnerability that entities within the public sector are lacking sufficient resources in relation to their area of responsibility and this increases the vulnerability of the Maltese system in relation to sanctions evasion and proliferation financing.

This leads to the following risk matrix, where the highest ranking is attributable to the vulnerability in view of the international nature of the financial transactions behind transhipment trade passing through Malta, Malta's geographical proximity to sanctioned countries coupled with Malta being a transhipment hub, the lack of sufficient technical knowledge or expertise by the subject persons Insufficient resources by the subject persons, and the sectors that are not required to have screening tools in place.

Table 103: Rating of vulnerabilities – PF and TFS

Vulnerability	Impact	Likelihood	Vulnerability level
The international nature of the financial transactions behind transhipment trade passing through Malta	Severe	High	High
Malta's geographical proximity to sanctioned countries coupled with Malta being a transhipment hub	Significant	High	Medium-high
Lack of sufficient technical knowledge or expertise by the subject persons	Severe	Moderate	Medium-high
Insufficient resources by the subject persons	Significant	Moderate	Medium-high
Sectors that are not required to have screening tools in place	Severe	Moderate	Medium-high
Insufficient resources in the regulatory authorities	Significant	Moderately low	Medium

13.3 Effectiveness of mitigating measures

This section presents a snapshot of all the mitigating measures in place by the competent and supervisory authorities, the law enforcement agency and the subject persons. In this area, the SMB is the national competent authority on sanctions, established by the National Interest (Enabling Powers) Act (NIA), Chapter 365 of the Laws of Malta, and is an autonomous body chaired by the Ministry for Foreign and European Affairs and Trade. The SMB liaises both with the private and public sectors on issues relating to sanctions and issues decisions thereon. Compliance with all UN/EU and national sanctions is governed by the NIA, which is a framework legislation for the implementation of sanctions under Maltese law. This law provides for the direct applicability of all UN and EU sanctions under national law without the need of any further legislation and ties any breaches of sanctions to hefty penalties which would be imposed by a Court of law following investigations by law enforcement authorities. Sanctions are covered by the NIA in their entirety, including any interpretations afforded to UN and EU texts through official guidelines and implementation assistance notices.

In the field of sanctions, most queries and cases handled by the SMB concern the Russia sanctions regime followed by Libya. In the case of Russia, the number of queries skyrocketed following the

new wave of sanctions against Russia as from February 2022. With regards to Libya, the close proximity of the country including the instance of Libyan frozen funds in Maltese financial institutions generate the greater number of queries and cases handled by the SMB. Most queries from the private sector relate to trade restrictions whilst queries submitted by financial institutions relate mostly to general questions on the interpretation of sanctions.

In light of the adoption of EU sanctions against Russia in February 2022, a thorough exercise was conducted by the MBR through its BO register of legal persons to identify any involvements of sanctioned individuals in Maltese incorporated legal persons. This process is undertaken in coordination with the SMB who shares lists of proposed listings at EU level with relevant stakeholders prior to their adoption. The MBR successfully identified a total of ten (10) Maltese registered legal persons having the involvement of sanctioned individuals and a total of twelve (12) legal persons which had been stuck off prior to the imposition of EU sanctions.

The NIA also requires all subject persons to screen client databases against the screening lists on a regular basis; have adequate systems in place to screen against applicable sanctions and enables the direct freezing of assets which belong to listed persons or entities or persons acting on their behalf. Subject persons are also to report the instances where targeted property is identified to the SMB and of the measures taken in relation to such property. UN and EU measures on sanctions and proliferation financing are thus directly applicable under Maltese law, notwithstanding that in the case of the latter, there is no specific mention per se. Any case of suspected sanctions evasion or proliferation financing would entail immediate freezing of the asset and reporting to the SMB. Thereupon the SMB would conduct further investigations and the matter is referred to law enforcement should a breach of applicable sanctions be deemed to have occurred. The SMB may dispose of any assets frozen/withheld or seized once a breach of sanctions is positively established, in any manner it deems fit.

Since the second quarter of 2019 risk profiles targeting countries subject to UN sanctions/EU restrictive measures were included in the Risk Management System ancillary to the Customs Export System. As a result, any customs export declaration with a country of destination being subject to sanctions, is being flagged to the STSMU. The need for constant monitoring for such transhipments is self-evident and includes the need to monitor transhipments of cargo below the controlled threshold. This is over and above the necessity on the part of Customs (MTCA) to monitor cargo destined for other countries using a risk-based approach.

With regards to supervision, there are a number of subject persons that are still to be supervised for sanctions to date. Meanwhile, from the supervisions that have been conducted, it was found that there are still gaps in compliance. Administrative fines were imposed mainly on CSPs, investment services companies and lawyers, for gaps in sanctions screening, followed by trustees and fiduciaries.

The following table presents the ratings of the effectiveness of mitigating measures of PF and TFS related risks, where the overall effectiveness is ‘substantial’. From the regulators point of view, moderate improvements are needed in terms of the supervision being carried out and the analysis of the transactional aspects. Minor improvements are needed with regards to outreach and training and guidance, where these improvements are specifically needed for the DNFBPs and financial

remitters. With regards to the subject persons, moderate improvements are needed in relation to PF risks and typologies by the DNFBPs, financial remitters and the credit institutions, better risk understanding and thus leading to a higher quantity and higher quality suspicious reports.

Table 104: Rating of effectiveness of mitigating measures – PF and TFS related risks

Controls put in place by regulators	
Level of dissuasiveness of final enforcement measures after appeal for breaches of CFT obligations	Moderate
CFT obligations, CFT guidance and outreach, level of CFT supervision, national cooperation between the authorities, fitness and proper checks.	High
AML/CFT controls by subject persons	
Reporting of STRs	Moderate
Reporting to SMB	Substantial
Risk understanding, assessment and management	Moderate
Resources dedicated to PF and sanction screening and staff knowledge	Substantial

13.1 PF and TFS residual risk

As indicated in the below table the overall residual risk of PF and TFS related risks is that of 'medium', with the residual risk being driven by the risk of money transfer services used to conduct cash transfers related to procurement of goods, and the risk of cross-border smuggling of cash to support proliferation activities.

Table 105: Residual risk ratings – PF and TFS related risks

Topic	Inherent risk	Effectiveness of mitigating measure	Residual risk	Overall residual risk level
Money transfer services used to conduct transfers related to procurement of goods	Medium-high	Moderate	Medium-high	**Overall residual risk = 'Medium'**
Cross-border smuggling of cash to support proliferation activities	Medium-high	Substantial	Medium-high	
Use of trade finance products and services in procurement of proliferation-sensitive goods	Medium-high	Substantial	Medium-high	
Use of personal banking accounts to purchase industrial items	Medium-high	High	Medium	
Use of front companies with opaque ownership structures to obtain trade finance products and services as parties to clean payments	Medium-high	High	Medium	
Use of legal persons registered in Malta with the BO hailing from sanctioned countries to mask parties to transactions and end users	Medium-high	High	Medium	

Use of vessels and/or shipping companies and/or the aviation industry in the movement of sensitive goods and/or to evade sanctions	Medium-high	High	Medium	
Nationals or dual citizens of proliferating states, or family members of such persons (regardless of citizenship), used as intermediaries in Malta to facilitate the procurement of goods and/or for payment	Medium-high	High	Medium	
Circumvention of sanctions through cryptocurrencies*	Medium-high	High	Medium	
Use of shell companies with the BO hailing from sanctioned countries, to obtain trade finance products and services as parties to clean payments	Medium	High	Medium-low	
Payments made to labourers (nationals or dual citizens) from North Korea, where these payments are then part of North Korea's revenue-raising activities	Medium	High	Medium-low	
Illicit Arms Trading	Medium	High	Medium-low	
Sale of minerals (gold, iron, steel, copper, and zinc) by North Korea or involving North Korean designated entities and individuals to raise revenue	Medium	High	Medium-low	
Exports originating from North Korea or involving North Korean designated entities and individuals	Medium	High	Medium-low	

**For a full analysis on the crypto assets to refer to section 10.3, where the analysis takes into consideration the licensed VFASPs in Malta, the unlicensed VFASPs in Malta, and the laundering through VFAs crypto currencies (regardless of where there is a VASP involved or its location) in Malta or by Maltese.*

13.2 Recommendations

The following recommended actions for subject persons are needed in order to continue addressing further the vulnerabilities in relation to the international nature of the financial transactions behind transhipment trade passing through Malta, Malta's proximity to sanctioned countries coupled with Malta being a transhipment hub, the lack of sufficient technical knowledge or expertise by the subject persons, the insufficient resources by the subject persons, and the vulnerability of having sectors that are not required to have screening tools in place. There is also the need to enhance the mitigating measures addressing the threat of money transfer services used to conduct cash transfers

related to procurement of goods, and the threat of cross-border smuggling of cash to support proliferation activities.

Update the PF risk understanding within the framework of their existing targeted financial sanctions and/or compliance programmes.

Align the policies, controls and procedures with the PF risk assessment
Consider introducing enhanced controls aimed at detecting and reporting possible breaches or evasion of targeted financial sanctions.

Measures should be commensurate with the level of risk, therefore, even where the risks are identified as lower in the PF risk assessment. This is in line with the FATF Guidance on Proliferation Financing risk assessment[120] that states that where there are higher risks, countries should require financial institutions and DNFBPs to take commensurate measures to manage and mitigate the risks. Where the risks are lower, they should ensure that the measures applied are commensurate with the level of risk, while still ensuring full implementation of the targeted financial sanctions as required by Recommendation 7[121]. By adopting risk-based measures, competent authorities, financial institutions and DNFBPs should be able to ensure that these measures are commensurate with the risks identified, and that would enable them to make decisions on how to allocate their own resources in the most effective way.

[120] Guidance on Proliferation Financing Risk Assessment and Mitigation (fatf-gafi.org)
[121] FATF Recommendation 7 requires countries to implement targeted financial sanctions to comply with the United Nations Security Council Resolutions (UNSCRs) relating to the prevention, suppression and disruption of proliferation of weapons of mass destructions (WMD) and its financing.

14 Summary of the results of the 2023 NRA

The following table summarises 2023 NRA results. The table by itself is not a substitute to a full understanding of the risks and their mitigation as described in full detail in this iteration of the NRA.

Table 106: Summary of the overall residual risk ratings: ML, TF, and PF and TFS related risks

Risk assessment	Inherent risk	Effectiveness of mitigating measure	Residual risk level
Money Laundering			
Financial sector			
Banking	Medium	High	Medium
Financial Institutions	Medium-high	Substantial	Medium-high
Investment services	Medium	Moderate	Medium
Pensions	Medium	Moderate	Medium
Insurance	Medium-low	High	Medium-low
DNFBPs			
Gaming			
Remote gaming	Medium-high	High	Medium
Land-based gaming	Medium	High	Medium
Recognition notice framework	Medium-high	Moderate	Medium-high
CSPs (including trustees and fiduciaries)	Medium-high	Substantial	Medium-high
Accountants and auditors	Medium-high	High	Medium
Lawyers	Medium	Substantial	Medium[122]
Tax advisors	Medium-high	Moderate	Medium-high
Dealing in immovable property	Medium-high	Substantial	Medium-high
Dealing in high value goods	Medium-high	Substantial	Medium-high
VFASPs	Medium-high	High	Medium

[122] As shown in table 16, the residual risk rating related to legal persons: Assisting in ML through the planning or carrying out of transactions for clients concerning the organization of contributions necessary for the creation, operation, or management of legal persons, has a 'medium-high' residual risk rating.

Money Laundering of the proceeds of:			
Domestic drug trafficking	Medium-high	Substantial	Medium-high
Local organized crime	Medium-high	Substantial	Medium-high
Foreign organised crime	Medium-high	Substantial	Medium-high
Foreign crime: fraud (including cybercrime)	Medium-high	Substantial	Medium-high
Corruption in Malta	Medium	High	Medium-low
Domestic tax crime	Medium	High	Medium-low
Foreign tax crime	Medium-high	High	Medium
Foreign crime: corruption	Medium	Substantial	Medium
Foreign crime: drug trafficking	Medium	Substantial	Medium
Domestic fraud	Medium	Substantial	Medium
Other instruments			
Legal persons	Medium-high	High	Medium-high
Legal arrangements	Medium-high	High	Medium
Citizenship & residency by investment schemes	Medium-high	High	Medium
Voluntary Organisations (NPOs)	Medium-high	High	Medium
ML typologies			
Abuse of Maltese registered legal persons with no sufficient links to Malta, for ML or concealment of BO	High	Substantial	Medium-high
The use of cash and cash-based businesses	High	Substantial	Medium-high
Trade based ML abusing geographical location and transhipment activity	Medium-high[123]	Substantial	Medium-high
Abuse of complex corporate structures for ML or concealment of BO	Medium high	Substantial	Medium-high
Laundering through high-value movables[124]	Medium-high	Substantial	Medium-high
Laundering through immovable property transactions	Medium-high	Substantial	Medium-high

[123] This rating is based significantly on an inherent threat of this international phenomena, rather than on specific TBML indicators found in Malta.
[124] Including through hire purchase agreement or leasing.

Abuse of Maltese registered legal persons as conduits in VAT fraud	Medium-high	High	Medium
Cross border cash activity	Medium	Substantial	Medium
Laundering of foreign proceeds of fraud through remote gaming operations	Medium	Substantial	Medium
Terrorist Financing[125]	Medium-high	High	Medium
Movement of funds for TF via financial institutions (remitters)	High	Substantial	Medium-high
Involvement of Maltese registered legal persons with BOs in HRJ (with no business relationship with the financial sector in Malta)	High	Substantial	Medium-high
Movement of funds for TF via cash cross-border movements	Medium-high	Substantial	Medium-high
Raising/Movement of funds for TF via disbursements of VOs (NPOs) that fall under the FATF scope[126]	Medium-high	High	Medium
Movement of funds for TF via credit institutions	Medium-high	High	Medium
Movement of funds for TF via cryptocurrencies	Medium-high	High	Medium
Trade-based TF	Medium-high	High	Medium
PF and TFS risks	Medium-high	High	Medium
Money transfer services used to conduct transfers related to procurement of goods	Medium-high	Moderate	Medium-high
Cross-border smuggling of cash to support proliferation activities	Medium-high	Substantial	Medium-high
Use of trade finance products and services in procurement of	Medium-high	Substantial	Medium

[125] Not all the topics are included here. For the full table refer to table 101.
[126] Only around 3% (55 out of 1,708) of the enrolled VOs (NPOs) with the OCVO are considered as falling under the scope of FATF recommendation 8.

	proliferation-sensitive goods			
	Use of personal banking accounts to purchase industrial items	Medium-high	High	Medium
	Use of front companies with opaque ownership structures to obtain trade finance products and services as parties to clean payments	Medium-high	High	Medium
	Abuse of legal persons registered in Malta to mask parties to transactions and end users	Medium-high	High	Medium
	Use of vessels and/or shipping companies and/or the aviation industry in the movement of sensitive goods and/or to evade sanctions	Medium-high	High	Medium
	Nationals or dual citizens of proliferating states, or family members of such persons (regardless of citizenship), used as intermediaries in Malta to facilitate the procurement of goods and/or for payment	Medium-high	High	Medium

15 List of acronyms

AIF	Alternative Investment Fund
AIP	Application Interface Program
AIFM	Alternative Investment Fund Manager
AML	Anti-Money Laundering
API	Advance Passenger Information
ARB	Asset Recovery Bureau
ATM	Automated Teller Machine
BIS	Bank for International Settlements
B2C	Business to Customer
BO	Beneficial Owner
BORIS	Beneficial Ownership Registers Interconnection System
CASPAR	Compliance and Supervision Platform for Assessing Risk
CBAR	Centralised Bank Account Register
CBI	Citizenship by Investment
CBM	Central Bank of Malta
CDD	Customer Due Diligence
CDD/KYC	Customer Due Diligence/Know Your Customer
CFT	Counter Terrorism Financing
CIS	Collective Investment Scheme
CMSI	Central Mediterranean Security Initiative
CPF	Counter Proliferation Financing
CPI	Corruption Perceptions Index
CRS	Common Reporting Standard
CSA	Court Services Agency
CSP	Company Service Provider
DLT	Distributed Ledger Technology
DNFBPs	Designated Non-Financial Businesses and Professions
DPRK	Democratic Republic of Korea
EBA	European Banking Authority
ECB	European Central Bank
ECSP	European Crowdfunding Service Providers
ECU	Economic Crimes Unit
EDD	Enhanced Due Diligence
EEA	European Economic Area
EIO	European Investigative Order
EMI	E-money Institutions
EU	European Union
EU SNRA	European Union Supranational Risk Assessment
FATCA	Foreign Account Tax Compliance Act
FATF	Financial Action Task force

FCC	Financial Crime Compliance
FCID	Financial Crimes Investigations Department
F&P	Fitness and Proper
FI	Financial Institution
FIAU	Financial Intelligence Analysis Unit
FIU	Financial Intelligence Unit
FTE	Full-time equivalent
GDP	Gross Domestic Product
GGR	Gross Gaming Revenue
GVA	Gross Value Added
HNWI	High Net Worth Individual
HRJ	High-risk jurisdictions
IIP	Individual Investor Programme
IMO	International Maritime Organization
KYC	Know Your Customer
LEA	Law Enforcement Authority
LOR	Letter of Request
MBR	Malta Business Registry
MER	Mutual Evaluation Report
MFE	Ministry for Finance and Employment
MFSA	Malta Financial Services Authority
MGA	Malta Gaming Authority
MIMIC	Multiple Indicators Multiple Causes
ML	Money Laundering
MLA	Mutual Legal Assistance
MLRO	Money Laundering Reporting Officer
MONEYVAL	Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism
MPF	Malta Police Force
MPRP	Malta Permanent Residence Programme
MSS	Malta Security Service
MTCA	Malta Tax and Customs Administration
NAIF	Notified Alternative Investment Fund
NAV	Net Asset Value
NCC	National Coordinating Committee on Combating Money Laundering and Funding for Terrorism
NCSI	National Cyber Security Index
NFT	Non-Fungible Token
NPO	Non-Profit Organization
NRA	National Risk Assessment
NSO	National Statistics Office
OAG	Office of the Attorney General
MTCA	Malta Tax and Customs Administration
OCGs	Organized Crime Groups
OCVO	Office of the Commissioner for Voluntary Organisations

OSA	Office of the State Advocate
OSINT	Open-Source Intelligence
PEP	Politically Exposed Person
PF	Proliferation Financing
PI	Payment Institutions
PIF	Professional Investor Funds
PMLA	Prevention of Money Laundering Act
PMLFTR	Prevention of Money Laundering and Funding of Terrorism Regulations
PNR	Passenger Name Record
P2P	Peer to Peer
RBI	Residency by Investment
RELB	Real Estate Licensing Board
RFA	Recognised Fund Administrators
RG	Responsible Gaming
RMA	Residency Malta Agency
RSA	Retirement Scheme Administrator
RUSI	Royal United Services Institute
SBI	Sports Betting Integrity
SDD	Simplified Due Diligence
SMB	Sanctions Monitoring Board
SMO	Senior Managing Official
SoF	Source of Funds
SoW	Source of Wealth
SAR	Suspicious Activity Report
SPV	Special Purpose Vehicle
STR	Suspicious Transaction Report
STSMU	Strategic Trade and Sanctions'. Monitoring Unit
SWG	Sectoral Working Group
TBML	Trade Based Money Laundering
TBTF	Trade Based Terrorist Financing
TCSP	Trust and Company Service Provider
TF	Terrorist Financing
TFS	Targeted Financial Sanctions
TM	Transport Malta
TRN	Transaction Report
TUBOR	Trust UBO Register
UBO	Ultimate Beneficial Owner
UCITS	Undertakings for Collective Investment in Transferable Securities
UK	United Kingdom
UN	United Nations
UNODC	United Nations Office on Drugs and Crime
VAT	Value Added Tax
VFAs	Virtual Financial Assets
VFASPs	Virtual Financial Asset Service Providers

VOs	Voluntary Organisations