Key results on the
Sectoral Risk Assessment of
Terrorism Financing and
National CFT Strategy

National Coordinating Committee on Combating
Money Laundering and Funding of Terrorism

December 2019

Table of Contents

Table of Figures

Acronyms used in this assessment

AML	Anti-Money Laundering
AMLU	Anti-Money Laundering Unit of the Malta Police Force
ARB	Asset Recovery Bureau
AGO	Office of the Attorney General
BO	Beneficial Owner
CBM	Central Bank of Malta
CVO	Commissioner for Voluntary Organisations
CPI	Transparency International Corruption Perception Index
CFT	Combating the Financing of Terrorism
CFP	Combating the Financing of Proliferation
EU	European Union
FATF	Financial Action Task Force
FI	Financial Institution
FIAU	Financial Intelligence Analysis Unit
FIU	Financial Intelligence Unit
GDP	Gross Domestic Product
IIP	Malta Individual Investor Programme
MBR	Malta Business Registry
MFSA	Malta Financial Services Authority
MGA	Malta Gaming Authority
MIIPA	Malta Individual Investor Programme Agency
MSS	Malta Security Service
ML	Money Laundering
MSB	Money Service Business
MLA	Mutual Legal Assistance
NCC	National Coordinating Committee on Combating Money Laundering and Terrorism Financing
NRA	National Risk Assessment
NPO	Non-Profit Organisations
OECD	Organisation for Economic Co-operation and Development
PF	Proliferation Financing
SMB	Sanctions Monitoring Board
STR	Suspicious Transaction Report
TF	Terrorism Financing
TFS	Targeted Financial Sanctions
VFA	Virtual Financial Asset
VO	Voluntary Organisation

1. Introduction

The Financial Action Task Force (FATF)[1] requires each country to identify, assess and understand the terrorist financing risks it faces in order to mitigate them and effectively dismantle and disrupt terrorist networks. FATF (2019) recommendation 1 lays out a number of basic principles with regards to TF risk. It calls on jurisdictions to "identify, assess and understand" the TF risks they face, including by designating "an authority or mechanism to coordinate actions to assess risk." [2] On the basis of this assessment, jurisdictions should apply a risk-based approach (RBA) to ensure that measures to prevent or mitigate TF are commensurate with the risks identified.

To this end, the National Coordinating Committee on Combating Money Laundering and Funding of Terrorism (NCC) was established within the Ministry for Finance through Subsidiary Legislation S.L. 373.02, enacted on the 13th April 2018. The NCC is the governing body responsible for the general oversight of Anti-Money Laundering and Countering the Financing of Terrorism (AML/CFT) policy. The NCC in 2018 led the exercise for the completion of thematic risk assessments, including for terrorism financing, the focus of this this paper. In fact, this paper presents the salient points emerging from this sectoral risk assessment which was a national effort and incorporated data and expertise from relevant authorities and the private sector. For competent authorities, the risk assessment will help prioritise efforts and resources using a risk-based approach. For the private sector, it will allow for the development of proportionate and effective controls.

Risk assessments are necessary, and this is especially so in view of the fact that the FATF guidelines[3] recommend that it is important that countries assess and continue to monitor their TF risks regardless of the absence of known threats. These guidelines stipulate that the absence of known or suspected terrorism and TF cases does not necessarily mean that a jurisdiction has a low TF risk. In particular, the absence of cases does not eliminate the potential for funds or other assets to be raised and used domestically (for a purpose other than terrorist attack) or to be transferred abroad. Jurisdictions without TF and terrorism cases will still need to consider the likelihood of terrorist funds being raised domestically, the likelihood of transfer of funds and other assets through, or out of, the country in support of terrorism, and the use of funds for reasons other than a domestic terrorist attack. Accordingly, section 2 of this paper presents an overview of the Maltese economy and how it has changed during the years, section 3 provides a description of the methodology adopted for assessing TF risk, while section 4 highlights the outcome of this assessment. Recommendations and concluding remarks are presented in section 5 and section 6 respectively.

---

[1] The Financial Action Task Force (FATF) is an independent inter-governmental body that develops and promotes policies to protect the global financial system against money laundering, terrorist financing and the financing of proliferation of weapons of mass destruction. The FATF Recommendations are recognised as the global anti-money laundering and counter-terrorist financing standard.

[2] FATF (2019), Terrorist Financing Risk Assessment Guidance, FATF, Paris, www.fatf-gafi.org/publications//methodsandtrends/documents/Terrorist-Financing-Risk-AssessmentGuidance.html

[3] FATF (2019), Terrorist Financing Risk Assessment Guidance, FATF, Paris, www.fatf-gafi.org/publications//methodsandtrends/documents/Terrorist-Financing-Risk-AssessmentGuidance.html

It is to be noted that ratings are not presented in this report given that as outlined in the EU Supranational Risk Assessment on Money Laundering (2017)[4], the rating itself is not a panacea. It only represents efforts to objectivize a line of reasoning by summarizing a complex analysis through a figure. Therefore, the report will not over-emphasize the risk rating, but will explain the material elements of the threats or the vulnerability that explain or justify the rating.

2. The Maltese economy

The required scope of a TF risk assessment will vary between jurisdictions, however, in line with the FATF guidance (2019), this may be impacted by: (i) the unique national and regional TF threat profile, (ii) the importance and materiality of different sectors, and (iii) the jurisdiction's geographic location and demographics. Accordingly, this section will assess the characteristics of the Maltese economy in order to highlight pertaining features of the Maltese economy.

The Republic of Malta is a Southern European island country 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 2018 of 493,559, up by 3.8 per cent when compared to 2017, making it one of the world's smallest and most densely populated countries. The population increase in 2018 was largely due to a net migration of 17,102 persons, an increase of 17 per cent when compared to the previous year. Excluding adoptions, the largest share of migrants were third-country nationals at 9,209 followed by other EU nationals at 7,349, with a net migration of Maltese nationals estimated at 480.[5]

Economic growth in 2018 reached 6.6 per cent in real terms, more than double the 1.9 per cent average rate of growth recorded by the EU-28. Malta is one of the fastest growing economies in the EU with a compounded rate of growth of 4.5 per cent between 2007 to 2018. As shown in Figure 1, the rate of growth recorded in 2007 to 2018 compares remarkably well with the EU average growth rate of 1.1 per cent. As a result, Malta's GDP per capita has increased from €15,500 in 2007 to €20,100 in 2018.[6]

[4] https://ec.europa.eu/info/files/supranational-risk-assessment-money-laundering-and-terrorist-financing-risks-affecting-union_en

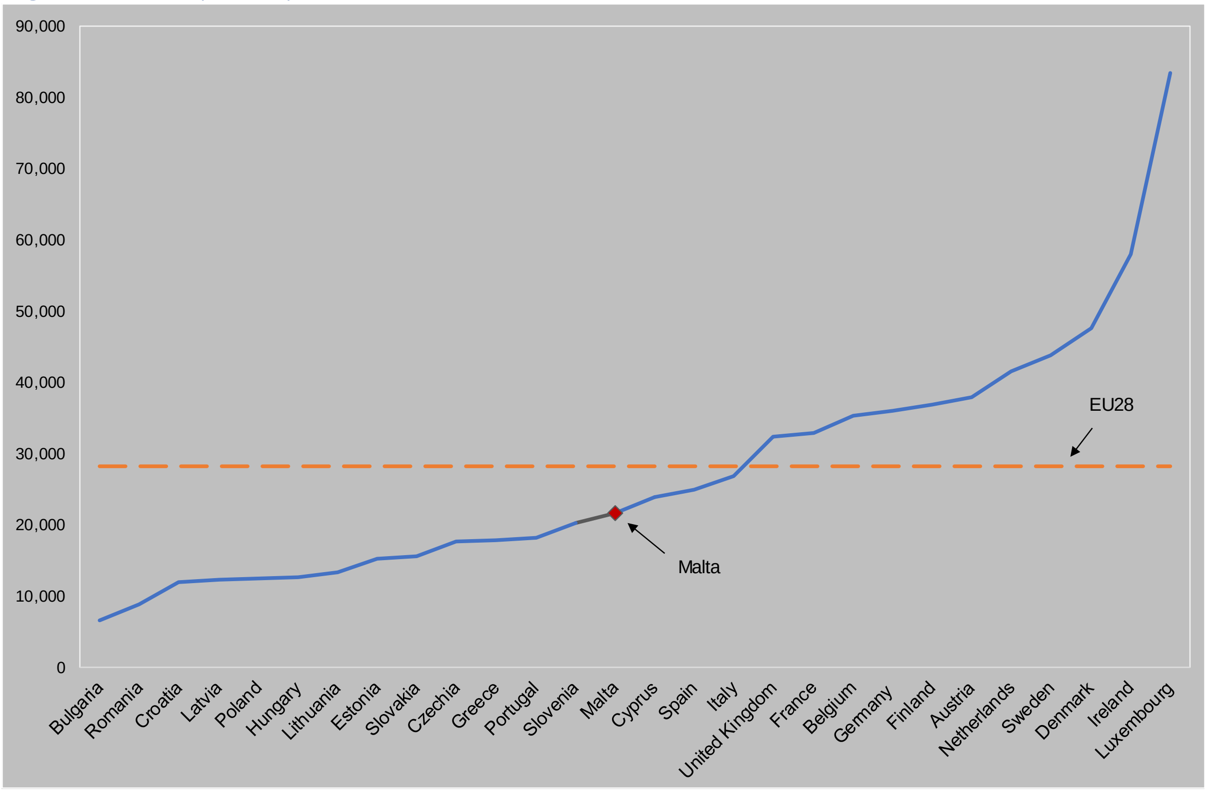
[5] Source: National Statistics Office

[6] Source: EUROSTAT

Figure 1: Malta and EU Real GDP growth (%)

Source: Eurostat

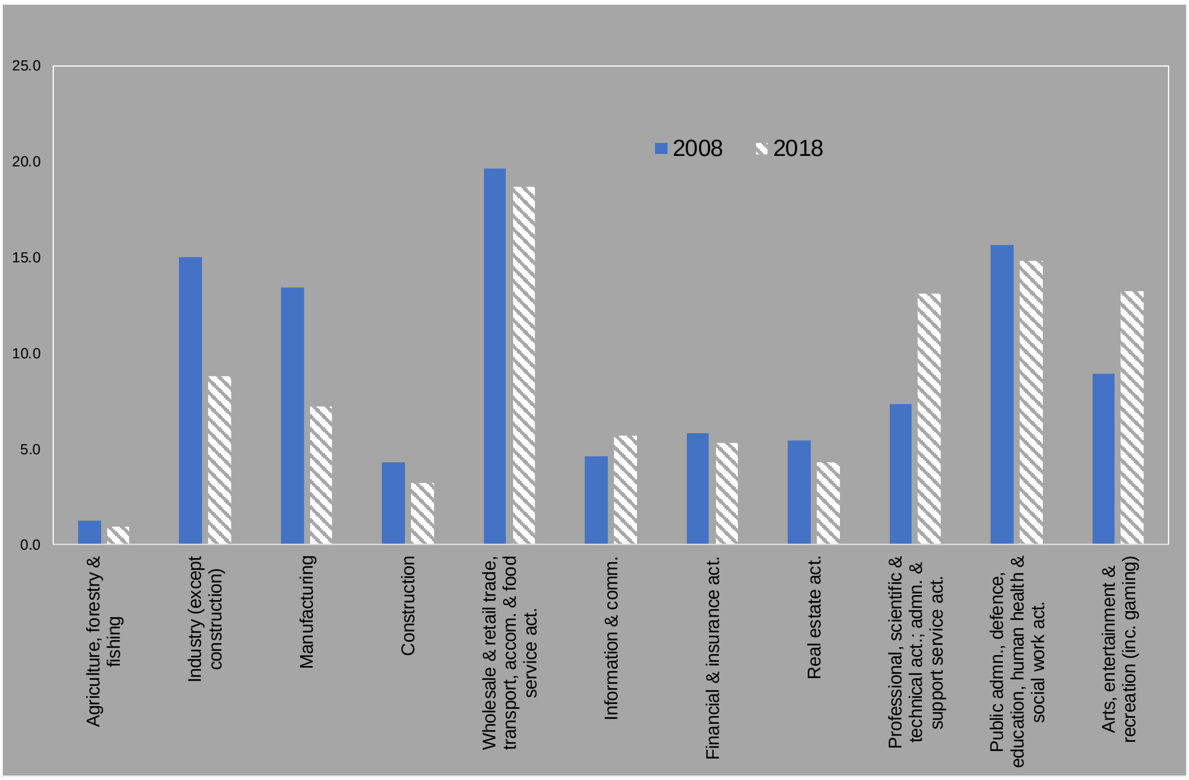
Figure 2: GDP per capita across EU Member States (Euro), 2018



Source: Eurostat

As shown in Figure 3, in the period from 2008 to 2018 in Malta there was a significant increase in the GVA as a percentage of the GDP originating from the professional sector that includes the legal and accounting professions and consultants as well as from the arts, entertainment and recreation sector that includes the gaming sector.

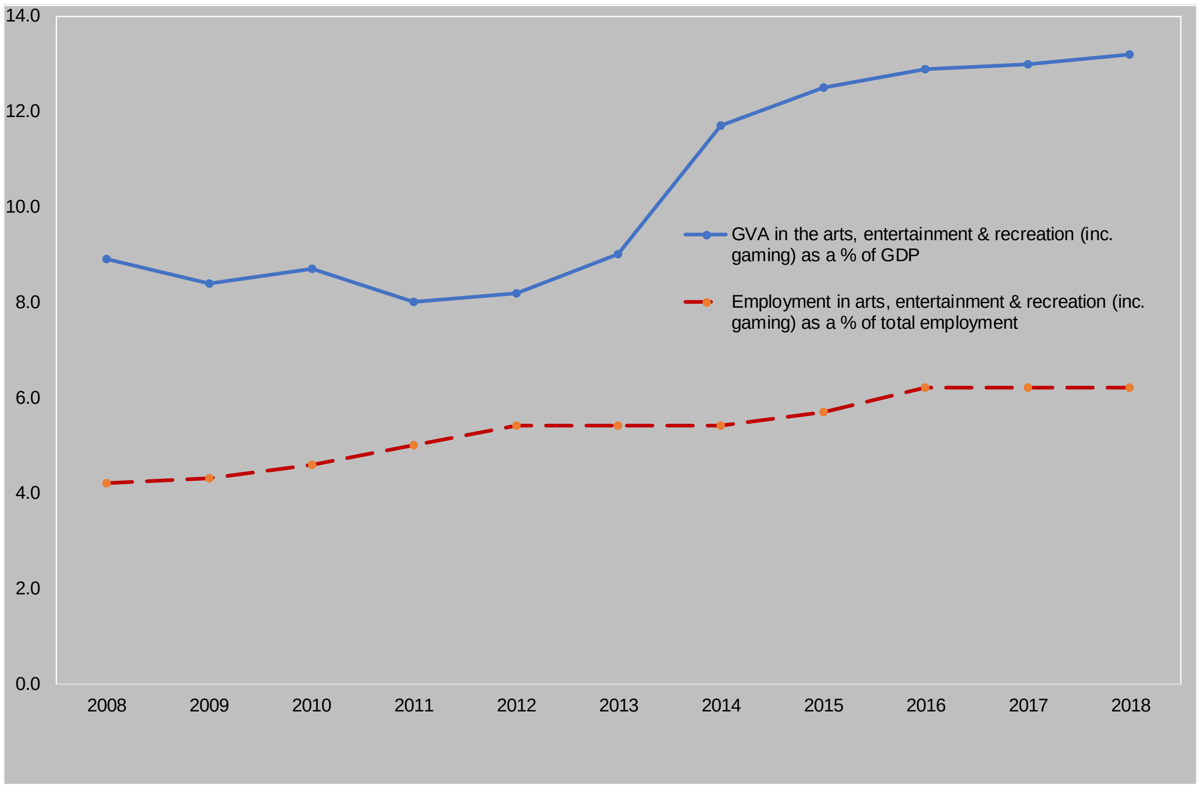
Figure 3: Gross Value Added by sector as a % of GDP (%)



Source: Eurostat

Furthermore, Figure 4 shows the growth pattern in the GVA and in employment in this latter sector as from 2008 to 2018. As shown in Figure 4, the gross value added from the arts, entertainment and recreation sector as a percentage of GDP increased from 8.9 per cent in 2008 to 13.2 per cent, whilst the percentage of employment in this sector increased from 4.2 per cent to 6.2 per cent during this same time period.

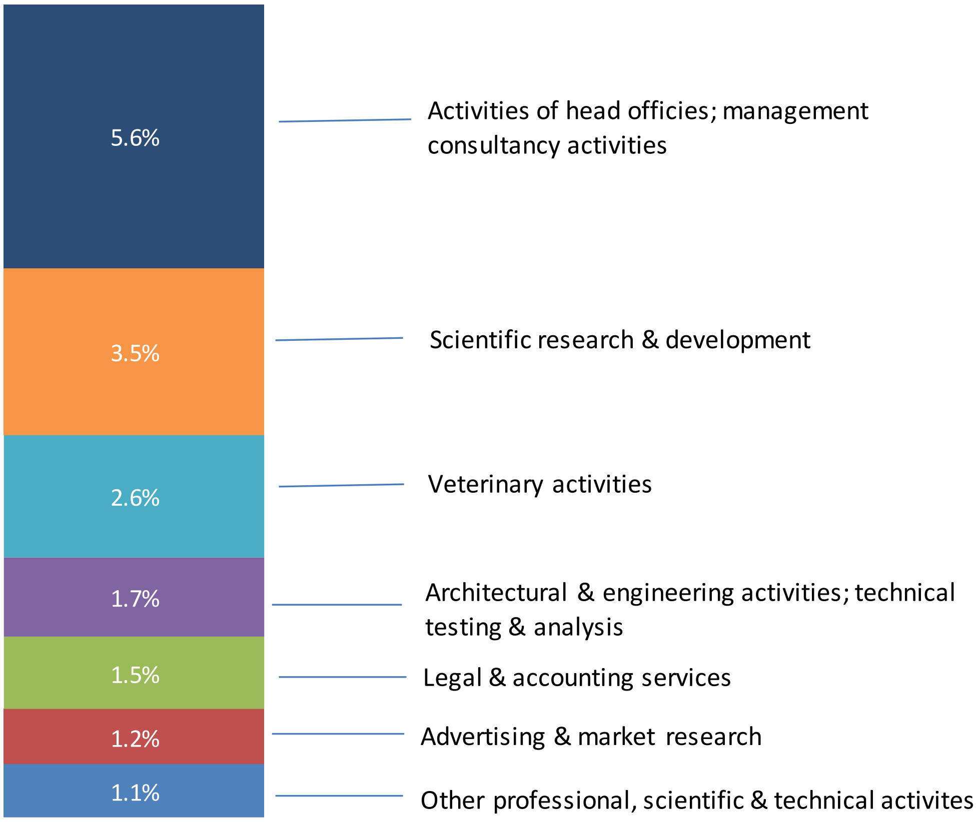
Figure 4: Breakdown of GDP and labour force in the arts, entertainment & recreation sector including gaming (%)



Source: Eurostat

As shown in figure 3 there was a notable increase in the GVA as a percentage of GDP originating from the professional sector. Accordingly, it is interesting to assess further this sector. Figure 5 shows the contribution increase of each component within this sector. In fact, according to this figure, 1.5 per cent of the increase in the Professional, Scientific and Technical activities in 2018 over 2017 is attributable to the Legal and Accounting Services sub-category.

Figure 5: The contributing growth in the 2018/2017 increase in the Professional, Scientific and Technical Activities (%)

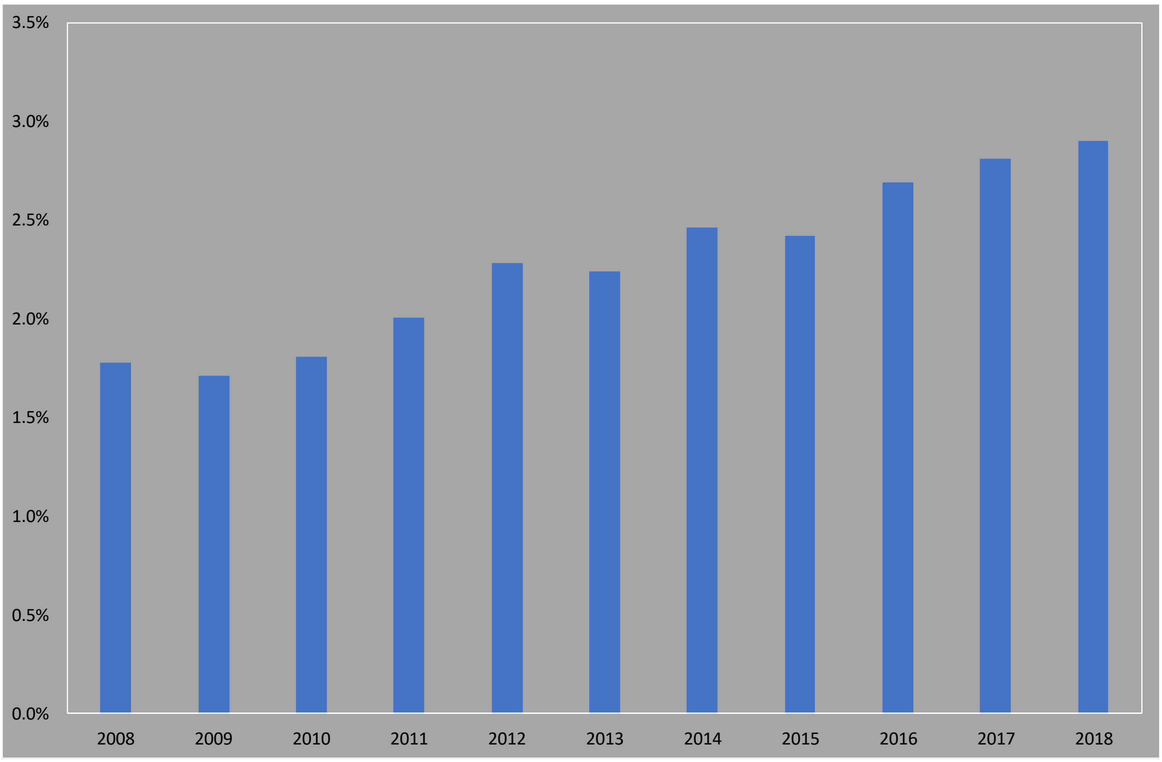


Source: National Statistics Office

Furthermore, in December 2018, full-time employment in the Legal and Accounting Services sub-category increased by 375 persons, an increase of 9.6 per cent over the comparable month in 2017. This is a notable increase and indicates the importance of this sub-category along the years. In fact, statistics from the Eurostat indicate that the employment share of the Legal and Accounting Services as a share of the Professional, Scientific and Technical Activities increased from 1.8 per cent in 2008 to 2.9 per cent in 2018 as shown in Figure 6 below. Given these developments it is interesting to assess in the next sections what threats and risks may have emerged in Malta as a result of these aspects.

.

Figure 6: Legal and Accounting Services as a share of the Professional, Scientific and Technical Activities (%)[7]



Source: Eurostat

What statistics indicate

In sum, growth in the services sector in Malta recorded significant increases and this as a result of the liberalisation measures, the higher availability of better educated labour resources and a targeted strategy to attract foreign direct investment. Besides the traditional areas of tourism, education, health, retailing and banking activities, the services industry expanded to include higher value-added activities generated by the financial services sector, specialised forms of tourism – like language schools and dive centres – maritime activity, professional services, back-office administration, information technology and gaming. Therefore, it is important that these emerging sectors are given the appropriate outreach programmes in order to mitigate the TF threats, vulnerabilities and risks that may be present. To understand this further, a definition of what in actual fact is a TF risk is provided in the next section.

[7] When compiling Labour Force Statistics for Eurostat, the NSO adopts the International Labour Organisation (ILO) definition, an internationally agreed definition on employment and unemployment. This definition has also been adopted by Eurostat and is used by all EU Member States. Since Jobsplus records and LFS results measure two different facets of employment and unemployment, these are not comparable. Users are therefore cautioned that these two sets of statistics should not be used interchangeably.

3. Definitions and approach taken

What is a TF risk?

According to the FATF guidelines (2019) countries often face particular challenges in assessing TF risks due to the low value of funds or other assets used in many instances, and the wide variety of sectors misused for the purpose of financing terrorism. TF shares many of the characteristics of ML, however, the factors associated with TF risk are distinct from those associated with ML risk. While laundered funds come from the proceeds of illegal activities, funds used to finance terrorism may come from both legitimate and illegitimate sources. Similarly, for ML it is often the case that the generation of funds may be an end in itself with the purpose of laundering being to transmit the funds to a legitimate enterprise. In the case of TF, the end is to support acts of terrorism, terrorist individuals and organisations, and for that reason the funds or other assets must, for the most part, ultimately be transferred to persons connected with terrorism. Another important distinction is that while identification of ML risk is often enforcement-led, TF risk by the nature of the threat will need to be more intelligence led.

A TF risk can be identified as being a function of three factors, that of threat, vulnerability and consequence. FATF guidelines point out that it involves the risk that funds or other assets intended for a terrorist[8] or terrorist organisation[9] are being raised, moved, stored or used in or through a jurisdiction, in the form of legitimate or illegitimate funds or other assets. According to the FATF guidelines, a TF threat is a person or group of people with the potential to cause harm by raising, moving, storing or using funds and other assets (whether from legitimate or illegitimate sources) for terrorist purposes. TF threats may include domestic or international terrorist organisations and their facilitators, their funds, as well as past, present and future TF activities, and individuals and populations sympathetic to terrorist organisations. On the other hand, the concept of TF vulnerability includes those things that can be exploited by the threat or that may support or facilitate its activities. Meanwhile, vulnerabilities may include features of a particular sector, a financial product or type of service that makes them attractive for TF. Vulnerabilities may also include weaknesses in measures designed specifically for CFT, or more broadly in AML/CFT systems or controls, or contextual features of a jurisdiction that may impact opportunities for terrorist financiers to raise or move funds or other assets. In addition, there may be some overlap in the vulnerabilities exploited for both ML and TF.

Furthermore, in the TF context, consequence refers to the impact or harm that a TF threat may cause if eventuated. This includes the effect of the underlying terrorist activity on domestic or institutional financial systems and institutions, as well as the economy and society more generally. Notably, consequences for TF are likely to be more severe than for ML or other types of financial crime (e.g. tax fraud etc.), which impacts how countries respond to identified threats.

---

[8] FATF (2019) stipulates that the term terrorist refers to any natural person who: (i) commits, or attempts to commit, terrorist acts by any means, directly or indirectly, unlawfully and wilfully; (ii) participates as an accomplice in terrorist acts ; (iii) organises or directs others to commit terrorist acts; or (iv) contributes to the commission of terrorist acts by a group of persons acting with a common purpose where the contribution is made intentionally and with the aim of furthering the terrorist act or with the knowledge of the intention of the group to commit a terrorist act.

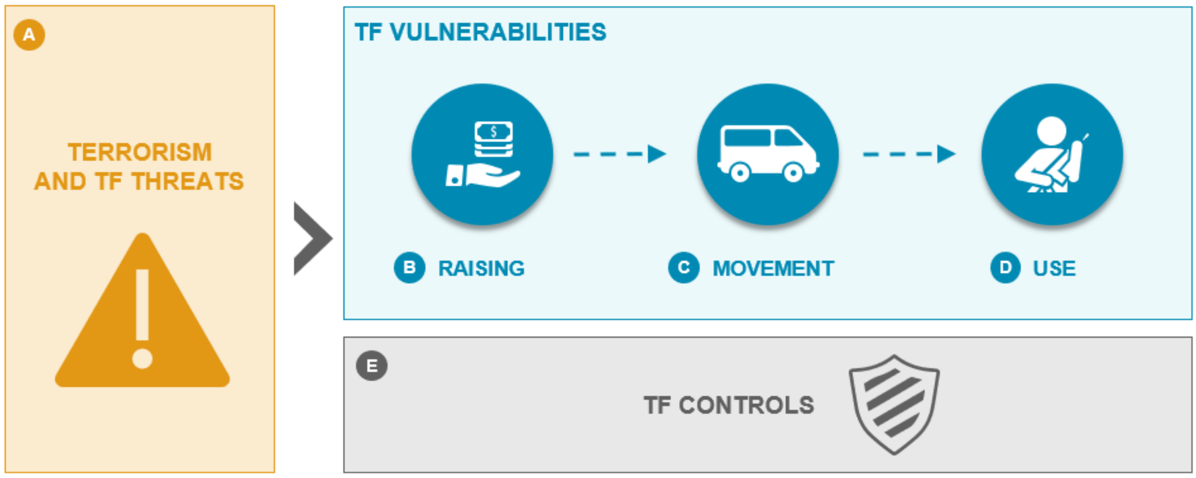
[9] FATF (2019) stipulates also that the term terrorist organisation refers to any group of terrorists that: (i) commits, or attempts to commit, terrorist acts by any means, directly or indirectly, unlawfully and wilfully; (ii) participates as an accomplice in terrorist acts; (iii) organises or directs others to commit terrorist acts; or (iv) contributes to the commission of terrorist acts by a group of persons acting with a common purpose where the contribution is made intentionally and with the aim of furthering the terrorist act or with the knowledge of the intention of the group to commit a terrorist act

Therefore, FATF guidance (2019) indicate that a TF risk assessment is a product or process based on a methodology, agreed by those parties involved, that attempts to identify, analyse and understand TF risk and serves as a first step in addressing them.

How is TF risk assessed?

While assessments may take different forms, a TF risk assessment should generally cover all aspects of raising, moving, storing and using funds or other assets (including goods, vehicles, weapons etc.) to meet the needs of a terrorist or terrorist organisation. Malta's TF risk assessment uses a framework that has been developed based on the Monaco Guidance[10], the latest FATF standards on CFT, and other international guidance (e.g. from the IMF). Developing this framework is necessary because there are important differences between TF and ML that mean the traditional ML framework (as used for Malta's NRA) must be adapted to comprehensively assess TF risks. Indeed, these two financial crimes are often very different. In fact, ML at the tactical end describes the process of making sums of dirty money appear legitimate, whereas TF attempts to use sums of (often legitimate) money for dirty purposes. The different elements adopted in this risk assessment are shown below.

Figure 7: TF risk assessment framework



[10] Monaco Workshop of Financial Centres, *Guidance on identifying, assessing and understanding the risk of terrorist financing in financial centres,* 2018

There are three main blocks to the framework – one covering threats, one covering vulnerabilities, and one covering controls. due to differences between ML and TF offences, the blocks have been adapted, such that the framework is made up of the five elements labelled A. – E. above, where:

- 'A' represents the ***threats*** in the context of TF refer to the actors that pose terrorism and TF threats to Malta. [11] This differs to the definition of threats in the ML context, which refers to predicate offences.
- ***Vulnerabilities*** in the context of TF refers to the three widely established methods of TF – raising, movement, and use of funds – that together form the end-to-end TF process. As stated in the Monaco Guidance, each of these must be considered in any assessment of TF risk.
    - 'B' implies the Raising Funds aspect which refers to the different sources that terrorist actors could use to fund their activities. These may be legitimate or illegitimate;
    - 'C' implies the Movement of Funds activity which refers to the channels or sectors that are at risk of misuse/abuse for facilitating the movement of terrorist funds;
    - 'D' refers to the Use of Funds which reflects the location where funds are most likely to be used.
- 'E' refers to the ***Controls*** in the context of TF refers to the overall CFT control environment. This incorporates the activities of both public and private sector stakeholders.

Neither threat nor inherent vulnerability are a judgement on the capability of a jurisdiction to combat TF. Both must take into account external factors (such as geography) which are not within the control of any jurisdiction; but are relevant for understanding context and must be considered when assessing the appropriate level of controls required. Each of the five elements (A. – E.) described above is addressed comprehensively in this assessment. However, in line with the Monaco Guidance, emphasis is placed on Malta's exposure to facilitating the cross-border movement of terrorist funds (C). This reflects the fact that 'the more likely exposure to TF for Financial Centres arises from their high levels of cross border business, particularly complex transactions, and the international activities of their charities and other non-profit organisations (NPOs)'. [12]

It is important to note that TF cases are hard to identify (in part due to low volumes required to fund a terrorist attack) and it is often difficult to categorically prove the link to terrorist activities. Therefore, the approach to assessing the inherent vulnerability is that:

- If an activity or sector is globally known to be used for TF, and a material volume is known to occur within a jurisdiction, it will be considered to be high vulnerability unless significant evidence to the contrary can be provided
- Lack of identified/ proved TF in an activity or sector is not accepted evidence due to the known challenges all jurisdictions face in identifying TF and the international immaturity of CFT measures

This approach is based on explicit FATF guidance on TF risk assessments.

[11] FATF (2016), *Consolidated FATF strategy for combatting terrorist financing*

[12] Monaco Workshop of Financial Centres, *Guidance on identifying, assessing and understanding the risk of terrorist financing in financial centres,* 2018

The key concepts, taken from the FATF guidance (2019) on money-laundering and terrorist financing risk assessment, are risk, threat, vulnerability and consequence, whereby:

- The risk element is based on the following major components for assessing each relevant sector:
    - The likelihood of terrorist groups or organized criminal groups misusing products or services provided by a sector for illicit purposes (that is, level of threat).
    - The potential weaknesses of those same products or services that allow terrorist groups or organized criminal groups to misuse them for illicit purposes (that is, level of vulnerability).

- The weaknesses are assessed according to the following criteria:
    - Inherent risk exposure of the product or service due to its inherent characteristics (based on the product, geographical or customer risks)
    - Risk awareness of the sector and competent authorities that the products or services may be misused (organizational framework of the sector, availability of a risk assessment, level of suspicious transactions reporting)
    - Legal framework and controls in place (existing legal framework, current implementation of the controls and of the customer's due diligence requirements, level of cooperation with competent authorities)

Based on the FATF guidance on the TF risk assessment, the approach adopted to assess the inherent vulnerability is that:

- If an activity or sector is globally known to be used for TF, and a material volume is known to occur within a jurisdiction, it will be considered to be highly vulnerable unless significant evidence to the contrary can be provided;
- Lack of identified/proved TF in an activity or sector is not accepted evidence due to the known challenges all jurisdictions face in identifying TF.

- A consequence is the impact or harm that terrorist financing may cause and includes the effect of the underlying criminal and terrorist activity on financial systems and institutions, as well as the economy and society more generally. The consequences of terrorist financing may be short- or long-term in nature and also relate to populations, specific communities, the business environment, or national or international interests, as well as the reputation and attractiveness of a country's financial sector.

According to the FATF guidance (2019), once jurisdictions have identified known and potential TF threats and vulnerabilities, the next step is to consider how these interact to form risks. The level of the country-inherent risk is calculated by combining an assessment of the level of threats taking into account the weaknesses of the financial system and the economy. The inherent risk exposure which reflects the risk exposure before the mitigating measures are put in place, is assessed through the following:

- Product: speed and anonymity of transactions, delivery channels, volume of transactions, cash involvement, management of new technologies and payment methods;
- Customer: high-risk customers, management of beneficial owner risks;
- Geographical risk: high-risk areas, size of cross-border transactions.

However, it is to be noted that neither threat nor inherent vulnerability are a judgement on the capability of a jurisdiction to fight TF. Both must take into account the external factors (such as geography) as well as the threats and vulnerabilities which are not within the control of any jurisdiction; but are relevant for understanding context and must be considered when assessing the appropriate level of controls required. Accordingly, the next section will proceed in highlighting the outcomes of this risk assessment.

4. Salient points

TF threats for Malta

Prior to addressing the TF threats indicated for Malta, it is important to point out that terrorism and TF threats are distinct; however, they are often interlinked. An understanding of the general terrorism environment and how it drives, and influences TF activity is therefore important in any TF risk assessment.[13] Similar to any other country, Malta faces threats from several different types of actor. These were identified as:

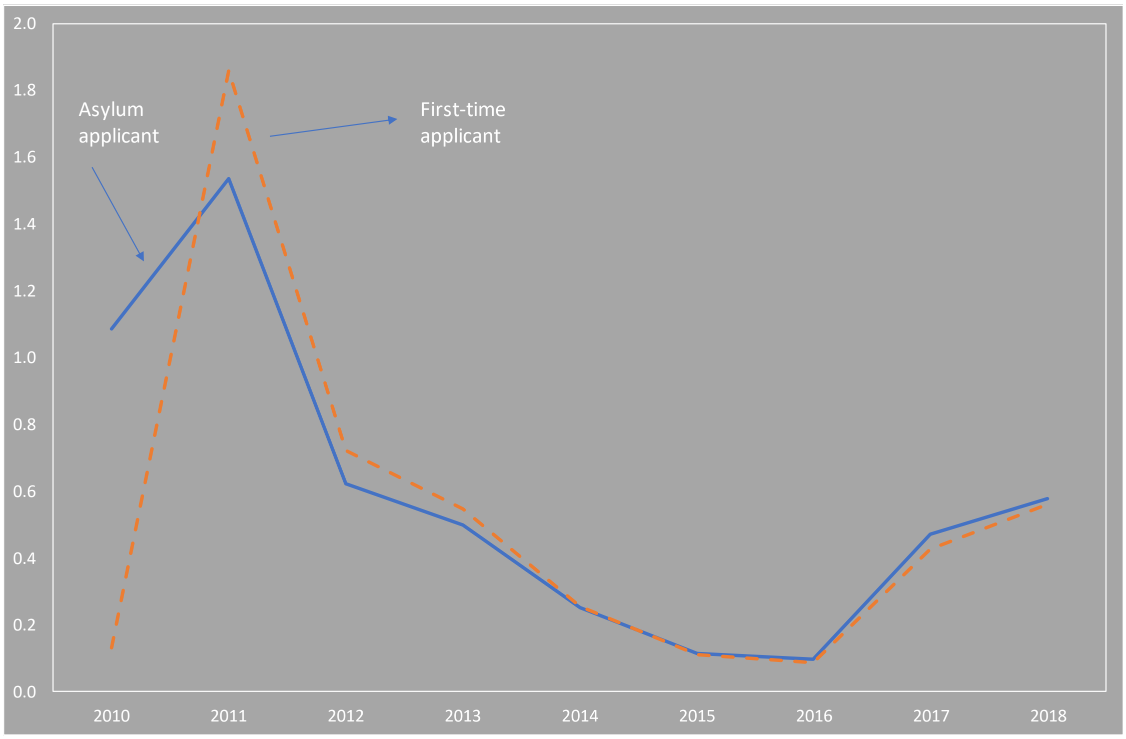
- small terrorist cells and lone actors - Individuals or small groups who typically rely on modest resources to carry out relatively low-tech attacks, for example, foreign terrorist fighters; small terrorist cells; and individual actors.
- command and control terrorist networks - organisations that seek to operative over an extended period of time, coordinating members' activities across the world;
- terrorist organisations which control significant territory - organisations that control territory or conduct military-like operations, and have organisational structures that more closely resemble that of armies and governments than terrorist cells;
- foreign safe havens and state sponsors of terrorism - nation states that 'repeatedly provide support for acts of international terrorism', or 'provide a safe haven for terrorist groups' (as defined by the US State Department List), for example, Syria, Iran, Sudan, Democratic People's Republic of Korea (DPRK), Libya, Iraq, Lebanon, Egypt; and
- 'corporate' terrorist groups - organisations that sit in the increasingly overlapping arena of terrorism and organised crime, for example, narco-terrorists, modern pirates.

Small terrorist cells and lone actors

In Malta, terrorist activity by small cells and lone actors has not been common. However, Malta has recently experienced levels of migration and refugee flows that are high relative to the size of the population – in particular from conflict zones in the Middle East and Africa as indicated in Figure 8 and Figure 9.

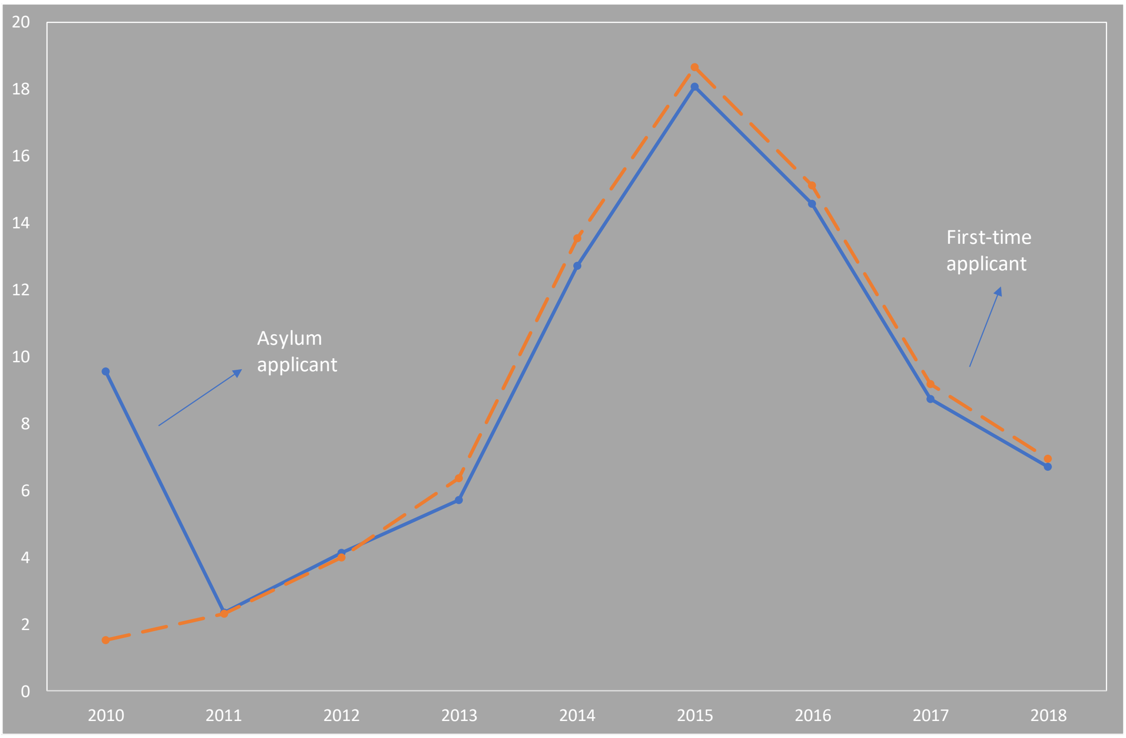
[13] FATF Risk Trends and Methods Group, *Draft terrorist financing risk assessment guidance,* 2019

Figure 8: Malta's share of the EU's asylum applicant and first-time applicants in Malta from Syria



Source: Eurostat

Figure 9: Malta's share of the EU's asylum applicant and first-time applicants in Malta from Libya



Source: Eurostat

Therefore, this implies that although there is currently no evidence to suggest these flows include individuals engaged in terrorist activities, in line with FATF guidance, this constitutes an important contextual factor in the consideration of TF threats. In addition, according to the Royal United Service Institute (2017), the nature of financing by small cells and lone actors, means that it is very difficult to prevent would-be terrorists from obtaining the trivial amounts of funding required for an attack. For example, the amount required to conduct an attack typically falls below cross-border cash declaration thresholds, which means that funds can be legally moved internationally without detection. Therefore, whilst the potential vale of fundraising is low, so are the opportunities to detect such financing prior to an attack. This creates a challenge for all the countries, even those such as Malta where there is a very limited history of terrorist activity.

Command and control networks

There is no recent history of terrorist attacks linked to these networks in Malta, however their presence in Malta's neighbouring countries remains. The transnational nature of command and control networks creates a need to move money internationally, and the methods used to do so are typically significant exposures for financial centres. As identified in the Monaco Guidance, these channels are material TF exposures for financial centres such as Malta.

Terrorist organisations which control significant territory

The primary areas of operation of these organisations is an important contextual factor for Mediterranean countries such as Malta. By definition, these organisations operate across vast swathes of land, currently focused in the Middle East (e.g. Iraq, Syria, Afghanistan) and Africa (e.g. Yemen, Libya, Tunisia) and whilst international efforts have led to a significant reduction in their territory, these organisations are still highly active in geographies bordering the Mediterranean. This drives a threat to all Mediterranean countries, even those where there has been limited terrorist activity to-date. Foreign safe havens and state sponsors of terrorism also create an enabling environment for TF. According to the US State Department, "in addition to their role in raising funds", safe havens and state sponsors "are important in how terrorists move and use finance". Therefore, this puts an extra threat and should be viewed in a way that caution is exercised.

Foreign safe havens and state sponsors of terrorism

Foreign safe havens and state sponsors of terrorism are nation states designed by the US State Department that "repeatedly provide support for acts of international terrorism" and/or allow terrorist groups "to organize, plan, raise funds, communicate, recruit, train, transit and operate in relative security". Forms of support vary considerably, and the identification of particular examples are often subject to political dispute, however there are several common themes. This risk assessment highlights that for Malta, Libya has been designated by the United States as a terrorist safe haven, and there are close economic links between the countries. As well as Libya's close geographical proximity to Malta, there are strong economic links between the countries which increasingly add emphasis to the element of threat present in our country.

'Corporate' terrorist groups

Terrorist attacks by these groups have not typically been in areas close to Malta. However, their involvement in international drug trafficking operations poses a TF risk to countries such as Malta. This is due to the potential for maritime infrastructure to be used as a transit destination in any such activity, and for the financial sector to be used to launder any process from this crime. In the Mediterranean, drug trafficking has been identified as a material TF exposure, partly due to the growing links between organised crime groups and terrorist organisations. Accordingly, this is an additional threat for our country.[14]

Concluding remarks

These threats should be viewed in relation to the fact that the FATF guidance (2019) stipulate that jurisdictions bordering a conflict zone or within close proximity to jurisdictions with active terrorist organisations often face additional cross-border TF threats. Malta's position within the Mediterranean poses a threat on its own and it is true that such a fact cannot be changed. Accordingly, it is important that authorities and entities understand the seriousness of the threats that are by their very nature impossible to prevent and have in place efficient and effective security checks in order to act beforehand.

TF vulnerabilities for Malta

Subsequent to identifying the threats, the risk assessment considers Malta's inherent vulnerabilities across the end-to-end TF process (raising, movement, and use of funds). In assessing this process, it is important to keep in mind, that the analysis focuses exclusively on Malta's exposure to TF and does not consider the effectiveness of controls. These vulnerabilities primarily relate to where the country's infrastructure (e.g. the Malta Freeport) or organisations (e.g. those in the financial services sector) could be used as a transit destination in the financing of terrorist activities overseas.

Raising Funds

Research indicates that terrorist actors raise funds from a range of sources, including both legitimate and illegitimate activities. In Malta, prior to any consideration of the controls that are in place, TF vulnerabilities relate primarily to the potential for the country's infrastructure (i.e. the Malta Freeport) to be used as a transit destination in illicit activities originating overseas.

Illegitimate sources of funds

When assessing illegitimate sources of funds, the focus was on funds intended for terrorist activities that are raised through activities that are in themselves illicit (i.e. generated through predicate offences), such as smuggling, drug trafficking, fraud and misappropriation, local and foreign criminal groups, fraud and misappropriation, and 'other' sources of funds.

- With regards to smuggling and drug trafficking, in Malta the inherent vulnerability primarily relates to the potential for the country's infrastructure to be used as a transit destination in activity originating overseas. In the Mediterranean smuggling has been identified by UNODC as a material TF exposure, which may be attributable to the growing links between the organised crime groups and the terrorist organisations. In Malta, this aspect that the country can be used as a transit destination acts as a significant inherent vulnerability. Furthermore, if one takes into account the fact of the known presence of terrorist groups in Libya, their tendency to raise funds via fuel smuggling and their historical control over port cities such as Sirte, then this draws a significant level of TF exposure to Malta.
- With regards to local and foreign criminal groups, in Malta the inherent vulnerability is driven by the known presence of local and foreign criminal groups in Malta, and their tendency to engage in activities that are important methods of raising funds (e.g. drug trafficking, fuel-smuggling). Globally, terrorist organisations form alliances with organized

[14] United Nations Office on Drugs and Crime, Drug trafficking and the financing of terrorism, 2018.

crime groups, including for the purpose of raising funds. In the Mediterranean, the links between terrorist organisations and organised crime groups have been identified by the UNODC as a material concern. The fact that in Malta both local and foreign organised criminal groups are known to operate is a vulnerability in terms of TF. In addition, the activities that criminal groups in Malta engage in are common fundraising methods for terrorist organisations such as fuel smuggling, narco-trafficking, and smuggling of counterfeit supplies such as cigarettes, and illegal immigration for example. However, although this highlights a significant vulnerability to TF it is important to highlight that there is minor evidence of long-standing and systematic alliances related to Malta.

- Furthermore, this risk assessment indicates also that in Malta, the element of fraudulent activity in the country, typically does not involve nationals of higher risk organisations and is therefore unlikely to be linked to TF. Globally, FATF indicates that fraud and misappropriation provide significant fundraising opportunities for terrorist organisations. This can take many different forms, including fraud related to credit cards, insurance, loans and tax. FATF research indicates also that courier and vishing frauds (a type of telephone scam) have also proved a popular fundraising method, particularly for those in Europe raising financing to travel to conflict zones in the Middle East. In these cases, vulnerable individuals are informed via telephone that bank accounts have been in some way compromised and are persuaded to transfer money into accounts controlled by the perpetrator, or to withdraw cash physically that is then collected from the victims' home by a courier.[15] However, in Malta, it was found that this inherent vulnerability is not so significant, given the fact that whilst there has been fraudulent activity in the country, this typically does not involve nationals of higher risk jurisdictions and therefore is unlikely to be linked to TF.
- With respect to 'other' sources of funds, for Malta it was found that despite the fact that there may be an element of risk that the country could be used as a transit destination in any human trafficking activity linked to TF given its geographical position, the risk assessment concludes that the nature of kidnapping for ransom and extortion are unlikely to occur given that these will take place in Malta.

Legitimate sources of funds

Meanwhile, legitimate sources of funds refer to funds intended for terrorist activities that are raised through activities that are not in themselves illicit, for example, fundraising through voluntary organisations, funding through legitimate business activities, self-funding, and direct contributions by groups or private donors.

- In Malta, the inherent vulnerability with respect to the fundraising through VOs is significant due to the high number of VOs (~1,600 are enrolled with the CVO) and the high number that have been designated as high-risk from an economic crime perspective (~185 have been designated as high risk or very high risk with 88 in high risk jurisdictions).
- The inherent vulnerability related to funding through legitimate business activities in Malta is driven by the prevalence of cash intensive businesses in the economy; the prevalence of business ownership by foreign nationals; and the size of sectors likely to be used to raise funds for terrorist actors. Malta has a large number of business, typically sole traders, who operate in a cash intensive economy. There are also the cultural aspects to take into consideration whereby it is common to pay by cash. Despite the fact that there are these cultural notions, it is to be noted that for risk assessment purposes, this high-level use of cash creates the opportunity to conceal illegitimate activity such as ML/TF because of the anonymity provided by using cash as a payment method. In addition, Malta has a high level

[15] FATF (2015), Emerging terrorist financing risks.

of business ownership by foreign nationals and this may include those from jurisdictions designated as terrorist safe heavens or state sponsors of terrorism. This is more pronounced when the ownership is that of Libyan nationals given that Libya is considered as a designated terrorist safe haven. Therefore, there is this added inherent vulnerability in our system.

- For Malta, the inherent vulnerability with regards to self-funding is due to the threat posed by small cells and lone actors and the difficulty in pre-emptively detecting and preventing their financing activities. Globally, this fundraising is either used to perpetrate cheap, low-tech attacks or to cover the costs of travel to join terrorist organisations located in conflict zones. According to FATF (2015) the most common funding sources are the salaries, social benefits from unemployment to family allowances, not paid-off consumer loans, overdrafts from multiple bank accounts, small donations from family, friends and supporters.[16] Thus, the inherent vulnerability in this case lies in the fact that it is difficult to pre-emptively detect and prevent such activity and this is what must be thoroughly understood.
- Then, with regards to the direct contributions by groups or private donors, the inherent vulnerability in Malta is not significant and there is no known evidence to suggest that such activity is taking place.

Movement of Funds

The movement of funds assessment considers potential channels in Malta which may be misused and/or abused to move terrorist funds. Terrorist actors use a range of channels to move funds within and across borders. Reflecting the Monaco Guidance[17], these channels have been broken down into three categories:

- Flow-through: relating to instances when the financial centre is used as a transit country for funds (or other stores of value) intended for use in foreign terrorism, for example:
  - credit institutions – exposure is driven by the size of the sector relative to GDP and the significant number of customers from high-risk countries. Credit institutions are one of the most important channels that terrorist actors use to move funds across the world, with the size and global operations of the banking sector providing opportunity to blend significant amounts of TF with legitimate international transactions. In addition, in recent years, several high-profile cases have highlighted vulnerabilities associated with branches or subsidiaries located in high-risk jurisdictions. Given that Malta has a large banking sector relative to the size of its GDP particularly when compared to other EU countries, then this creates significant opportunity for terrorist actors to blend movement of funds within a high level of legitimate banking activity. Furthermore, Malta is an international financial sector and processes high levels of payment transactions, many of which ‘pass through’ its credit institutions and do not have any substantive link to the country. Thus, it is to be noted that there is a significant element of inherent vulnerability in terms of credit institutions.
  - payment institutions, e-money institutions and other value transfer mechanisms – exposure is driven by the level and nature of money remittance activity, specifically the high value of remittances and the high-risk nature of their source and destination. This category involves (i) payment and e-money institutions that are licensed in Malta by the MFSA under the Financial Institutions Act; (ii) the payment and e-money

[16] FATF (2015), Financing of the terrorist organisation Islamic State in Iraq and the Levant (ISIL).

[17] Monaco Workshop of Financial Centres, *Guidance on identifying, assessing and understanding the risk of terrorist financing in financial centres,* 2018

institutions that are not licensed in Malta but can legally service Maltese customers due to reciprocal arrangements; (iii) unlicensed value transfer mechanisms that operate illegally in Malta.

  - Globally, money remittance services provide a common and convenient method for terrorist actors to move money and can offer rapid transfer of funds with a high-level of anonymity. Such remittance services provide a channel to obscure the movement of terrorist funds within a high-level of legitimate activity. Misuse and abuse of remittance services typically occur where regulation is weaker and/or where service providers themselves are complicit.
  - Globally, internet-based payment and e-money services are increasingly used to move money across borders and as such represent an emerging TF risk. In Malta, there is a high value of remittances, and the high-risk nature of remittances source and destination are considered as an inherent vulnerability and imply that entities need to be cautious in their operations in this regard and aware of the risks that their operations may entail.

- couriers and other cash transfer mechanisms – exposure is driven by the extent of cash use in the economy and the level of cash movement into Malta from high-risk jurisdictions. Such frequency of cash transactions means that carrying cash is not particularly uncommon and is viewed as an opportunity for terrorist actors to move funds under the disguise of legitimate activity. Vulnerabilities associated with physical movement of cash are most significant in economies with a high degree of cash usage and/or where terrorist organisations are known to carry out their core activities. Therefore, even for Malta, such a high frequency of cash transactions implies that carrying cash is not particularly uncommon and provides opportunity for terrorist actors to move funds under the guise of legitimate activity.
- new and emerging payment technologies – exposure is driven by the scale of recent and expected future growth of the virtual financial assets sector;
  - Pre-paid cards represent an increasing TF vulnerability and are replacing travelers cheques as a method of moving money offshore. Whilst a variety of pre-paid card types exist, the category of most concern is those that are 'open-loop' and allow funds to be withdraw from ATMs worldwide. In particular, open-loop General Purpose Reload (GPR) cards are a significant vulnerability. These GPR cards can be obtained online or from various retailers and are then activated and 'loaded' with funds (e.g. online or by phone) post-purchase. Thereafter they function like any other bank-issued debit card. The anonymity and flexibility make pre-paid cards particularly attractive for TF purposes. Open-loop GPR cards can be 'loaded' domestically using cash or other non-reportable electronic methods and can be carried offshore without requirement to declare across the border. On arrival, the funds can then be converted back into cash by terrorist actors, restricted only by ATM withdrawal limits. Such cards are also flexible – for example, some systems allow several cards to be linked to a common set of funds, meaning a third party can load funds using one card, and beneficiaries overseas (who need only the card and PIN to access funds) can withdraw using a separate linked card. In addition, pre-paid card providers often fall below AML/CFT regime thresholds and so are not subjected to client due diligence (CDD) requirements, making it difficult to link a card back to a natural person.
  - Two features of virtual currencies make them particularly attractive for those looking to move terrorist funds – firstly, anonymity of both users and transactions; secondly, their ability to move funds quickly from one country to another.

    - other financial service providers – whilst some exposure is driven by the size of the insurance and securities, this risk assessment does not indicate that this is a significant vulnerability;
    - legal entities and arrangements (excluding financial services) – exposure is driven by the large number of private companies, their complex beneficial ownership structures and the concentration of ownership in foreign individuals.

- Service providers: relating to instances when businesses in the financial centre provide admin/other services to parties supporting terrorism, for example:
    - DNFBPs (excluding gaming)- exposure is driven primarily by the size of the legal and accounting professions and the international nature of their clientele.
    - Gaming – exposure is driven by the size of the remote gaming sector in relation to the size of the Maltese economy. Whilst the remote gaming sector is large relative to the size of Malta's economy, this risk assessment concludes that the likelihood of misuse and/or abused that facilitates the movement of terrorist funds is not significant.

- Abuse of philanthropic organisations: relating to instances when donations/aid sent to, or administered by, financial centres are diverted to support foreign terrorism, for example the voluntary organisations, which in Malta are quite high in number along with the fact that there is a high number that have been designated as high-risk from an economic crime perspective. 'Diversion of funds' is the most common typology for misuse and abuse of such organisations for terrorism and TF purposes. Within the 'diversion of funds' typology there are two broad categories of misuse and abuse – that by internal actors and that by external actors. The diversion of funds by internal actors accounts for the majority of cases studied in FATF reports whereby internal actors are well positioned to divert funds for immoral purposes. A wide variety of techniques for moving funds are observed, including wire transfers; cash transfers and couriers; travelers cheques; MSBs; and accounts of unrelated persons/businesses. On the other hand, as indicated by FATF reports, the diversion of funds by external actors is relatively less common, and in such cases third-party associates of the non-profit organisation (e.g. external fundraisers or foreign funds) divert funds that are destined for, or provided by the non-profit organisation. Examples include instances where intermediaries such as MSBs deduct a 'tax' to be passed onto terrorist organisations; and where beneficiaries of charitable funds are themselves 'taxed' by terrorist groups.

Like many other financial centres, there are several channels in Malta that are particularly exposed to TF. The nature of these exposures typically relates to facilitating cross-border movement of funds intended for use overseas. The primary drivers of this are the vulnerabilities associated with credit institutions; payment institutions, e-money institutions and other value transfer mechanisms; couriers and other cash transfer mechanisms; voluntary organisations, and the new and emerging payment technologies (such as virtual currencies). Again, it is important to highlight that such considerations reflect Malta's exposure or susceptibility to TF and at this point do not incorporate any consideration of control effectiveness.

Use of funds

Any terrorist funds that are raised in Malta, or moved through Malta, could be used for a variety of different purposes and in numerous different locations. It is very difficult to ascertain specific uses of funds and therefore this part of the assessment considered more broadly whether any funds that may be raised in/moved through Malta would be more likely to be used domestically or internationally. As an international financial centre the possibility of facilitating international use of funds is more significant. This is primarily due to the high-level of cross-border transactions facilitated by Malta, and the significant level of financial flows to countries where terrorist activity is taking place.

In fact, the vulnerabilities assessment of the domestic use of funds, highlights that the risk that any funds raised in or moved through Malta will be used for terrorist activity domestically is low. There have however been a significant number of terrorism-related fatalities in neighbouring countries in North-East Africa and the Middle East in the past years, as well as the high-level of activity in fellow EU member states (there were 205 attacks in EU countries in 2017), which lead to some level of exposure for Malta. Despite the high-level of activity in neighbouring countries and fellow EU member states, Malta has a very limited history of terrorist activity in the country, and the current threat level has been determined as low.

On the other hand, the risk that any funds raised in or moved through Malta will be used for terrorist activity overseas is set as significant by this assessment. This is driven by three factors: (1) the exposure of Malta as an international financial centre to high volumes of cross-border transactions that may include terrorist funds destined for use overseas; (2) significant financial flows between Malta and places where terrorist activity is taking place; and (3) recent cases of the Maltese financial system potentially being used to move terrorist funds for use overseas (e.g. in relation to credit institutions and money remittance services). The Monaco Guidance highlights that the extent of financial transactions flowing through these jurisdictions makes it likely that this could include terrorist funds that are then used overseas – "the more likely exposure…arises from their high levels of cross border business, particularly complex transactions…with the attendant possibility of the services and products offered by financial centres or assets raised and/or disbursed by their non-profit organisations being used by parties outside the jurisdiction to fund terrorism abroad".

Effectiveness of controls

The risk assessment then considers the effectiveness of Malta's controls to combat TF. Given that Malta's CFT controls are varied, numerous and implemented by a diverse range of stakeholders, they are grouped into three broad categories for this assessment: prevention (excluding law enforcement);[18] supervision; and intelligence, investigation, prosecution, and asset recovery.

With regards to prevention, the assessment describes the controls implemented by public and private sector stakeholders to prevent terrorist funds from being raised, moved or used. These controls include the actions taken by six main stakeholders: Customs, SMB, MIIPA, MBR and the Private Sector. These six stakeholders implement a range of controls to prevent TF, notably including Malta's cross-border cash declaration regime; legal obligations to adhere to UN and EU financial sanctions; a four-tier due diligence process for any person applying for citizenship through the IIP; and numerous preventative measures carried out by the private sector pursuant to their AML/CFT obligations. In this assessment, the following areas have been identified as priorities for improvement: (1) improve operational arrangements and legislative framework for cross-border cash control regime; (2) address challenges in verification processes for ultimate beneficial ownership information; (3) improve understanding of TF risks and knowledge of CFT and TFS obligations among the private sector; (4) improve use of advanced analytics for ongoing monitoring by the private sector (which contributes to relatively low

[18] Note, this grouping excludes controls implemented by law enforcement authorities and the use of financial intelligence – these are considered under "Intelligence, investigation, prosecution and asset recovery"

numbers of TF STRs); and (5) address inconsistencies in the robustness of CDD processes across the private sector.

With regards to the assessment on supervision this includes the actions of four main stakeholders: FIAU, MFSA, MGA, OCVO. These stakeholders conduct CFT supervision through measures including market entry controls; ongoing monitoring of compliance with CFT obligations; the imposition of supervisory sanctions for non-compliance; and training and outreach to improve subject persons' understanding of TF risks and CFT obligations. Since the development of Malta's National AML/CFT Strategy, significant work has been undertaken to strengthen these controls, including increasing resources and developing new risk rating tools and processes. However, the following areas have been identified as priorities for improvement: (1) address inconsistencies in understanding of TF risks among supervisors; (2) improve process for using ML/TF risk ratings to inform the nature and frequency of supervisory activity (requirement to build on recent strengthening activities); (3) improve market entry controls and ongoing risk-based supervision of certain DNFBPs (e.g. Real Estate); (4) more TF-specific outreach and guidance required; (5) increase focus on CFT and build shared learnings between AML/CFT and prudential supervision; and (6) increase number of resources dedicated to AML/CFT supervision.

With regards to the intelligence, investigation, prosecution and asset recovery this includes primarily the actions of six main stakeholders: FIAU, AMLU, CTU, MSS, AGO and ARB. These actions include the analysis and dissemination of financial Intelligence; the use of such financial information and additional counter-terrorism Intelligence to investigate TF cases; and the prosecution of these cases. This risk assessment has highlighted four areas that need further improvements: (1) potential to increase severity of legal framework for TF-related criminal sanctions; (2) development of CFT National Strategy required; (3) expand financial intelligence available; and (4) build experience in asset recovery.

The emerging outcome here is that while the authorities built the foundations of robust and effective CFT controls over the past years, the effectiveness of Malta's CFT end-to-end process needs to be further strengthened.

5. Recommendations

Based on the assessment of Malta's TF threats, vulnerabilities and controls, the NCC has identified eight thematic initiatives to strengthen the national CFT regime. These initiatives include new measures specific to CFT, as well as the development of existing measures already being implemented as part of the 2018 AML/CFT Strategy. The eight initiatives are:

- **Further develop and formalise the strategic approach to CFT at a national level**, through completing the National Counter Terrorism Strategy (and ensuring CFT is integrated within it); and by formalising inter-agency CFT coordination mechanisms;

- **Review the legal framework** around terrorism and TF, specifically considering whether sanctions for TF offences are sufficiently dissuasive;

- **Enhance understanding of TF risks and knowledge of CFT obligations and TFS obligations** through increased outreach to the private sector and VOs; reviewing options to establish a Public Private Partnership on AML/CFT; and further TF-related training for relevant public bodies;

- **Accelerate efforts to strengthen the AML/CFT supervisory framework** by investing in resources; continuing to strengthen links between prudential and AML/CFT supervision; strengthening the supervisory framework for certain DNFBPs; and continuing to develop the supervisory approach for VOs;

- **Review and strengthen the end-to-end process from analysis of TF intelligence to investigation of TF cases** by enhancing FIAU's access to relevant information; developing the tools and personnel to analyse this information; reviewing allocation of responsibilities and internal capabilities for TF investigation within the Police; and improving the effectiveness of cooperation between the Police and other authorities;

- **Accelerate efforts to strengthen the cross-border cash regime** through legislative changes that empower the Customs Department, as well as investment to enhance processes, tools, and personnel;

- **Continue to enhance processes and capabilities to verify beneficial ownership** by adopting and implementing the recommendations of Malta's Risk Assessment and Strategy for Legal Entities, Arrangements, and Voluntary Organisations

- **Accelerate efforts to establish an effective asset recovery unit** by implementing the relevant recommendations of Malta's National AML/CFT Strategy.

These thematic initiatives cut across the three categories of controls of prevention, supervision and intelligence, investigation, prosecution and asset recovery. The initiatives also call for different parts of the control framework to be enhanced. These parts of the control framework include:

- strategy, organisation and governance
- legal and regulatory framework
- capabilities and processes and
- data, systems and tools.

6. Implications for the private sector

This risk assessment emphasises the need for competent authorities to engage the private sector and help them understand TF risks and CFT obligations. To provide further guidance on the implications of this risk assessment for the private sector, some actions are articulated below:

- Develop and maintain an up-to-date internal risk assessment and use this to ensure that operations are in line with risk appetite. For private sector entities that are exposed to significant TF risks, this assessment should include explicit consideration of specific TF typologies;

- Develop a CDD methodology to ensure (potential) clients and their activities are appropriately risk profiled. Specifically, this should include enhancing KYC checks and ensuring that robust processes are in place to screen (potential) clients against TFS lists;

- Enhance processes for ongoing CFT monitoring and move beyond simple threshold-based transaction monitoring. Among larger and more sophisticated institutions, this should include developing the capabilities to conduct more complex network analysis that can identify suspicious patterns of activity in transactions and customer behaviour. Where possible in view of the nature and size of the activity, operators may consider deploying sophisticated AI and machine learning techniques to detect previously unidentified suspicious behaviour;
- Ensure that the number of STRs filed in relation to TF is consistent with the risk profile of the organisations. For larger and more complex organisations in higher risk sectors, this will mean an increase in the number of TF-related STRs filed with the FIAU;

- Review the appropriateness of controls to detect and prevent deliberate facilitation of TF by 'bad actors' within private sector organisations. This should include ensuring that adequate surveillance is in place to monitor staff, particularly in sectors that are more exposed to TF;

- Collaborate closely with competent authorities to ensure Malta has an effective national CFT framework. This should include providing rapid responses to information requests by FIAU and law enforcement in cases of potential TF; attending outreach workshops as relevant; providing feedback on guidance documents issued by supervisors (e.g. relating to TF and TFS); actively engaging to raise awareness of new and emerging TF risks; and sharing good practices (e.g. as part of cross-institutional private sector initiatives, or as part of public-private partnerships). For example, in the UK, private sector institutions and public sector bodies collaborate on AML/CFT as part of the Joint Money Laundering and Intelligence Taskforce.

7. Limitations in this risk assessment

Given the nature of terrorism and TF offences and lack of terrorist activity to date in Malta ultimately means that data was limited. The lack of known terrorism and TF incidents means that there is little available information that is specific to Malta. Information from numerous public sources including international bodies and research providers were used to help substantiate the report's conclusions and provide data for case studies. In addition, qualitative insights from key stakeholders were used to refine conclusions further. Where data was missing or unavailable, a prudent approach was taken to ensure that the level of risk was not under-stated. This is in line with FATF's guidance which is as follows

"Where information gaps exist or difficulties in reaching conclusions arise, it is useful if these can be recognised in the risk assessment and then become areas where more work is required in the future. In addition, the uncertainty caused by the lack of information may itself raise the risk profile of the issue under consideration. In seeking to develop a comprehensive picture, those in charge of the ML/TF risk assessment need to identify and acknowledge these limitations as they make a determination of the risks that can be assessed. Future risk assessments may be able to seek new or alternative sources of information that will permit assessment of areas that could not be adequately or fully assessed in an earlier work."[19]

[19] *FATF Guidance on National Money Laundering and Terrorist Financing Risk Assessment,* February 2013

Despite these limitations, NCC as the governing body responsible for the general oversight of AML/CFT policy, will continue to work hard to ensure that this risk assessment is continuously carried out and will provide a comprehensive, coordinated and communicated strategy for managing the risks, have an effective execution of and follow-through on decisions made, as well as effective ongoing cooperation and intelligence sharing among stakeholders, especially in light of the fact that risks are not static but are continuously changing.