FATF

FATF REPORT

Terrorist Financing Risk Assessment Guidance

July 2019

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 (AML) and counter-terrorist financing (CFT) standard.

For more information about the FATF, please visit **www.fatf-gafi.org**

This document and/or any map included herein are without prejudice to the status of or sovereignty over any territory, to the delimitation of international frontiers and boundaries and to the name of any territory, city or area.

Citing reference:

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

Table of contents

ACRONYMS

AML	Anti-money laundering
CFT	Countering the financing of terrorism
FSRBs	FATF style regional bodies
FIU	Financial Intelligence Unit
FTF	Foreign Terrorist Fighter
ISIL	Islamic State of Iraq and Levant
LEA	Law Enforcement Agencies
MEs	Mutual Evaluations
MONEYVAL	The Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism
MSB	Money Service Business
MVTS	Money Value Transfer Services
NRA	National Risk Assessment
NPO	Non-profit Organisation
TF	Terrorist Financing

EXECUTIVE SUMMARY

1. Terrorists regularly adapt how and where they raise and move funds and other assets in order to circumvent safeguards that jurisdictions have put in place to detect and disrupt this activity. Identifying, assessing and understanding terrorist financing (TF) risk is an essential part of dismantling and disrupting terrorist networks[1]. An understanding of TF risk should also inform national counter terrorist financing (CFT) strategies and assists in the effective implementation of a risk-based approach (RBA) towards CFT measures.

2. 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 TF purposes. The cross-border nature of TF can pose additional challenges for identification of risk. Moreover, the operational needs for attacks can include routine transactional activity (e.g. car rental, purchasing a kitchen knife). Lower capacity jurisdictions often face further challenges due to a lack of TF expertise or personnel, and information gaps on unregulated or unsupervised activities.

3. Building on the *FATFs 2013 Guidance on National Money Laundering and Terrorist Financing Risk Assessments*[2], this report provides good approaches, relevant information sources and practical examples for practitioners to consider when assessing TF risk at the jurisdiction level. This report draws on inputs from over 35 jurisdictions from across the FATF Global Network[3] on their extensive experience and lessons learnt in assessing TF risk. While all countries should have a holistic understanding of all stages of TF (raising, moving and use of funds or other assets), this report recognises that there is no one-size fits all approach when assessing TF risk. Jurisdictions will need to extract from this Guidance those parts that are most relevant to their unique context and threat profile.

4. This report covers: key considerations when determining the relevant scope and governance of a TF risk assessment, and practical examples to overcome information sharing challenges related to TF and terrorism information. This report provides examples of information sources when identifying TF threats and vulnerabilities, and considerations for different country contexts (e.g. financial and trade centres, lower capacity jurisdictions, jurisdictions bordering a conflict zone etc.). In addition, this report covers relevant information sources for practitioners when identifying TF risks within the banking and Money or Value Transfer (MVTS)

1 In October 2018, FATF completed work to identify good approaches and tools for disrupting terrorist financing activity based on specific examples provided by 33 jurisdictions from across the Global Network. FATF delegations have disseminated the relevant outcomes to competent authorities.

2 www.fatf-gafi.org/publications/methodsandtrends/documents/ml-tf-risks.html

3 **FATF:** Argentina, Australia, Belgium, Canada, China, Germany, Hong Kong China, Italy, Ireland, Israel, Malaysia, Mexico, the Netherlands, Norway, Russia, Singapore, Sweden, U.S., U.K; **APG:** Brunei Darussalam, Macao, China; Papa New Guinea, The Philippines, Vanuatu; **EAG:** Kyrgyzstan; **GAFILAT:** Costa Rica, Colombia, Guatemala, Nicaragua, Peru, Paraguay; **GIABA:** Nigeria; Ghana; **MONEYVAL:** Armenia; Monaco, Ukraine; **MENAFATF:** Lebanon.

sectors, as well as good approaches for assessing TF risks facing those Non-Profit Organisations (NPOs) which fall within the FATF definition[4].

5. While a risk assessment presents a snapshot in time, **this report highlights the importance of establishing regular mechanisms to monitor TF risk on an ongoing basis, taking into account current terrorism and TF threats and developments**. In light of the cross-border nature of TF, jurisdictions that face a low domestic terrorism risk may still face significant TF risks. Likewise, even countries that assess their TF risk to be low will still need to regularly monitor and review their understanding, and to stay vigilant to potential changes in TF threats and trends. **This report highlights the importance of continuing to critically reviewing the approach taken to assess TF risk, and identifying blind spots and areas where further information is needed**. For some jurisdictions, it may be necessary to take a phased approach to assessing TF risk, and to prioritise the establishment of a mechanism to gathering and collecting relevant quantitative and qualitative information.

6. Jurisdiction experience in assessing TF risk is continuing to evolve. This report concludes with some areas for further focus going forward based on experience from across the FATF Global Network, including enhanced information sharing on TF risks among jurisdictions with similar threat profiles, the continued development of multi-agency information sharing initiatives, and use of information technology tools to manage "big data."

[4] FATF defines an NPO as: "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.'"

INTRODUCTION

Purpose, Scope & Objectives

7. **Terrorists regularly adapt how and where they raise and move funds and other assets in order to circumvent safeguards that jurisdictions have put in place to detect and disrupt this activity.** Identifying, assessing and understanding terrorist financing (TF) risks is an essential part of dismantling and disrupting terrorist networks, as well as the effective implementation of the risk-based approach (RBA) of counter terrorist financing (CTF) measures.

8. **Developing and maintaining an understanding of evolving TF risks can often present unique challenges for jurisdictions.** The low value of funds or other assets used in many instances, and the wide variety of sectors misused for TF purposes, makes identification of TF vulnerabilities and threats challenging. Countries can also face challenges due to the limited availability of TF or terrorism information domestically, or the limited amount of criminal/intelligence cases under investigation. The lack of terrorism and TF expertise or personnel, and limited information on unregulated or unsupervised activities can pose further challenges for lower capacity countries. Due to such challenges, TF risk is often given limited attention in National Risk Assessments (NRAs) and is sometimes not differentiated from the risk of terrorism. Similarly, in developing a methodology for assessing risks, jurisdictions sometimes fail to take into account the unique threats posed by terrorist financiers and sympathisers as opposed to criminals.

9. **The objective of this report is to provide guidance and practical examples for jurisdictions on how to overcome some of these challenges.** Nevertheless, there should not be a one-size-fits-all approach in assessing TF risks. An effective approach for one jurisdiction will not necessarily be effective for others[5]. The scope, focus and objectives of a TF risk assessment will vary depending on a jurisdiction's unique threat profile, national context and wider counter terrorism (CT) and CFT activities and strategies. Recognizing this, the purpose of this report is to present good approaches taken by jurisdictions based on varying materiality, context and TF threat profiles. Countries will then need to extract from this Guidance those parts that are most relevant to its TF risk and context. In this regard, the country examples provided in this report are included for reference and their inclusion in the Guidance does not prejudge alternative approaches to assessing risk.

10. **The FATF Standards provide flexibility in how jurisdictions assess their TF risks, and do not proscribe a particular risk assessment methodology.** The scope of this report covers TF risk assessments conducted as part of broader NRAs, as well as the more specific assessments that are sometimes used to support NRAs (e.g. sectoral risk assessments, agency-specific risk assessments, assessments of high-risk corridor financial flows etc.). The objective of this report is not to analyse the key

[5] A developing country with large levels of informality and porous borders close to a conflict zone and that itself has suffered terrorist attacks may need to take a completely different approach compared to a developed country with a sophisticated financial sector that is not located anywhere near areas of conflict.

TF threats and vulnerabilities that other FATF reports have covered[6], but to support jurisdictions in improving the mechanisms used to understand these threats and vulnerabilities. While this report touches on potential follow-up actions after the completion of a TF risk, this report does not extend to the implementation of measures to address identified risks.

11. **This report builds on the FATF's previous work on risk assessments, specifically the 2013 *FATF Guidance on National Money Laundering (ML) and Terrorist Financing Risk Assessment*[7].** In particular, this report builds on the extensive experience that jurisdictions have had since the 2013 Guidance in conducting risk assessments, and focuses on the unique challenges in assessing TF risk (as opposed to ML risk). This report constitutes a reference for States undertaking to assess their TF risk as requested by UNSCR Resolution 2462 which was adopted in March 2019[8]. This report also takes into account work that other international bodies have carried out on this topic, such as the 2018 UNODC *Guidance Manual for Member States on Terrorist Financing Risk Assessments*[9]; and the *OSCE Handbook on Data Collection in Supporting ML and TF National Risk Assessments*[10].

Structure

12. The objectives of this report are delivered through six sections:

- ***Part 1: Governance, Scoping and National Coordination - Good Approaches and Considerations*** – This section presents considerations for competent authorities when determining the scope and coordination of a TF risk assessments, and provides practical examples to overcome domestic information sharing and coordination challenges.
- ***Part 2: Terrorist Financing Risk Methodologies - Good Approaches and Considerations*** – Recognising that there is no-one-size fits all approach when assessing TF risk, this section draws on the different risk methodologies used by over 35 jurisdictions from across the FATF Global Network, and identifies good approaches and relevant information sources.
- ***Part 3: Assessing Cross-border and Sector-specific Terrorist Financing Risks*** – This section presents jurisdiction experience in assessing cross-border TF risks, and relevant information sources for when assessing sector-specific TF risks within the banking sector and the Money Value Transfer Service(MVTS)/remittance sectors, as well as exploitation of natural or environmental resources.
- ***Part 4: Non-Profit Organisations (NPOs) and Assessing Terrorist Financing Risk*** - Recognising the unique FATF requirements for assessing TF

6 For an overview of past FATF work to identify threats and vulnerabilities, refer to the FATF public website.
7 www.fatf-gafi.org/publications/methodsandtrends/documents/ml-tf-risks.html
8 https://undocs.org/S/RES/2462(2019)
9 www.unodc.org/documents/terrorism/Publications/CFT%20Manual/Guidance_Manual_TF_Risk_Assessments.pdf
10 www.osce.org/secretariat/96398?download=true

risk among those NPOs that fall within the FATF definition[11], this section presents some good approaches and jurisdiction examples in assessing TF risk facing NPOs.

- ***Part 5: Follow up and Maintaining an Up-to-date Assessment of Terrorist Financing Risk*** **–** This section provides considerations and good approaches when communicating the findings of the TF risk assessment, and maintaining an up-to-date assessment of TF risk.
- ***Conclusion*** **–** The report ends with some areas for further focus going forward based on experience from across the FATF Global Network.

Methodology

13. **This report incorporates inputs from a number of delegations within the FATF Global Network that have carried out extensive work on assessing TF risk**. Over 35 FATF and FATF Style Regional Body (FSRB) members have submitted information and case studies on their experience in assessing TF risk at the sectoral, national and regional levels, as a means to identify best practice and common challenges[12]. The challenges and good approaches for assessing TF risk identified in this report also draw partly on a horizontal review of completed Fourth Round FATF and FSRB Mutual Evaluations (MEs).

14. An experts' workshop hosted jointly by the FATF and the Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism (MONEYVAL) was held in Tel Aviv, Israel in March 2019 to gather inputs for the report. The project team also held a targeted consultation with civil society representatives on the sidelines of the FATF Private Sector Consultative Forum in May 2019.

Key Concepts and Terms Relevant to Assessing Terrorist Financing Risk

15. In discussing TF risk assessments, it is necessary to have a common understanding of the key concepts. For the purpose of assessing TF risk (whether as part of an NRA or otherwise), this guidance uses the following key terms[13]:

- **A TF risk** can be seen as a function of three factors: threat, vulnerability and consequence. It involves the risk that funds or other assets intended for a

---

11 FATF defines an NPO as: "*a legal person or arrangement or organisation that primarily engages in raising or disbursing funds for purposes such as charitable, religious, cultural, educational, social or fraternal purposes, or for the carrying out of other types of "good works*". The FATF Recommendation 8 applies only to those NPOs that fall within this definition.

12 **FATF:** Argentina, Australia, Belgium, Canada, China, Germany, Hong Kong China, Italy, Ireland, Israel, Malaysia, Mexico, the Netherlands, Norway, Russia, Singapore, Sweden, U.S., U.K; **APG:** Brunei Darussalam, Macao, China; Papa New Guinea, The Philippines, Vanuatu; **EAG:** Kyrgyzstan; **GAFILAT:** Costa Rica, Colombia, Guatemala, Nicaragua, Peru, Paraguay; **GIABA:** Nigeria; Ghana; **MONEYVAL:** Armenia; Monaco, Ukraine; **MENAFATF:** Lebanon.

13 These terms draw on the definitions provided in the FATF 2013 Guidance on National ML and TF Risk Assessments.

terrorist[14] or terrorist organisation[15] are being raised, moved, stored or used in or through a jurisdiction, in the form of legitimate or illegitimate funds or other assets.

- A **TF threat** is a person or group of people[16] 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.
- The concept of **TF vulnerability** comprises those things that can be exploited by the threat or that may support or facilitate its activities. Vulnerabilities may include features of a particular sector, a financial product or type of service that makes them attractive for TF. Vulnerabilities may also include weaknesses in measures designed specifically for CFT[17], or more broadly in AML/CFT systems or controls, or contextual features of a jurisdiction that may impact opportunities for terrorist financiers to raise or move funds or other assets (e.g. large informal economy, porous borders etc.). There may be some overlap in the vulnerabilities exploited for both ML and TF.
- 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. Consequences of TF are also likely to differ between countries and between TF channels or sources, and may relate to specific communities or populations, the business environment, or national interests. Given the challenges in assessing consequences, countries need not take a scientific approach when considering consequences, and instead may want to start with

14 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.

15 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.

16 This may include both natural and legal persons.

17 In particular, FATF Recommendation 5 (R.5) and Recommendation 6 (R.6) set out in detail the specific requirements to criminalise TF and implement targeted financial sanctions on the basis of the *International Convention for the Suppression of the Financing of Terrorism (1999)* and *relevant UN Security Council Resolutions (UNSCRs).*

the presumption that consequences of TF will be severe (whether domestic or elsewhere) and consider whether there are any factors that would alter that conclusion.

- 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. **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.** This should go beyond the revenue raising aspects and address terrorist procurement and terrorist facilitation networks, including Foreign Terrorist Fighters (FTFs).

How is terrorist financing risk different from terrorism risk?

16. **TF risk and terrorism risk are often, but not always, interlinked.** For example, an assessment of TF risk will require a consideration of the domestic and foreign terrorist threats. If a jurisdiction has active terrorist organisations operating domestically or regionally, this will likely increase the probability of TF. **Nevertheless, in light of the cross-border nature of TF, a jurisdiction that faces a low terrorism risk may still face significant TF risks.** A low terrorism risk implies that terrorist individuals and groups are not using funds domestically for terrorist attacks. However, actors may still exploit vulnerabilities to raise or store funds or other assets domestically, or to move funds or other assets through the jurisdiction.

17. **Crucially the factors associated with TF risk are also 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.

18. **Although there may be some overlap in the potential vulnerabilities that criminals and terrorists misuse, the motive, and therefore the threat and risk indicators, differs.** While transfer of a low volume of funds may be lower risk for ML, this type of activity may pose a higher risk indicator for TF when considered along with other factors (e.g. reporting thresholds or limited amount of funds necessary to carry out terrorist acts). For example, terrorist financiers have been known to use low-limit prepaid cards for TF purposes despite being considered lower risk for ML (see pages 36-37 of *FATF Report on Emerging TF Threats*[18]).

18 www.fatf-gafi.org/media/fatf/documents/reports/Emerging-Terrorist-Financing-Risks.pdf

Core FATF Obligations Regarding Assessing Terrorist Financing Risk at the Jurisdiction-level

19. **This section provides a brief outline of the FATF Requirements with respect to TF risk identification and assessment at the jurisdiction-level**[19]. Importantly, the risk-based approach is a key component of the Fourth Round FATF Standards, and a jurisdiction's risk and context are critically relevant to evaluating technical compliance with FATF Recommendation 1, as well as assessing effectiveness across a number of FATF Immediate Outcomes.

- **Recommendation 1 (R.1):** R.1 lays out a number of basic principles with regard 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 co-ordinate actions to assess risk." 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.
- **Interpretative Note to Recommendation 1 (INR.1**[20]**):** INR.1 clarifies that jurisdictions should take steps to identify and assess their TF risks on an "ongoing basis" in order to: (1) inform potential changes to the jurisdiction's AML/CFT regime, including changes to laws, regulations; and (2) assist in the allocation and prioritisation of AML/CFT resources by competent authorities. Jurisdictions should have a mechanism to provide information on the results of the risk assessment(s) to all relevant competent authorities and self-regulatory bodies (SRBs), financial institutions, and designated non-financial businesses and professions (DNFBPs).
- **Recommendation 8 (R.8):** R.8 includes the TF requirements applicable to those NPOs that fall within the FATF definition. The requirements under R.8 are exclusively focused on TF and do not extend to ML. The risk-based approach is an essential component of R. 8. For further detail on the R.8 risk requirements, see Chapter 4 below.
- **Effectiveness in Implementing the FATF Standards:** A jurisdiction's TF risk assessment and understanding is also considered under FATF Immediate Outcome 1 (IO.1), and impacts the extent to which a jurisdiction effectively meets the objectives across a number of other Immediate Outcomes[21]. IO.1 considers:
    - ***Involvement of all relevant competent authorities:*** the extent to "which competent authorities and relevant stakeholders (including financial

[19] For more details, reference should be made to the text of Recommendation 1 and its Interpretive Note, as well as the FATF Methodology.

[20] Footnote 1 of INR. 1 specifically acknowledges that supra-national risk assessments should be taken into account, where appropriate.

[21] Most notably, TF risk understanding impacts the extent to which jurisdictions can effectively identify and investigate TF cases (Immediate Outcome 9), deprive terrorists and terrorist organisations of assets and instrumentalities related to terrorist activities, and prevent them from abusing the NPO sector (Immediate Outcome 10); and provide guidance to reporting entities on TF risk (Immediate Outcome 3 & 4).

institutions and DNFBPs) are involved in risk assessment", "how they provide inputs, and at what stage?" and whether "adequate resources and expertise were involved."

- ***Engagement with non-government stakeholders*:** the extent to which the jurisdiction ensures that respective financial institutions, DNFBPs and other relevant sectors are aware of the relevant results of the national TF risk assessment(s) (e.g., *through briefings and guidance on relevant conclusions from risk assessment(s); input to develop risk assessment(s) and other policy products*).
- ***Quality of information sources***: the comprehensiveness of the methods, tools, and information used to develop, review and evaluate the conclusions of the assessment(s) of risks.
- ***The reasonableness and timeliness of the TF risk assessment***: the timeliness of the risk assessment, and the extent to which the risk assessment is reasonable and consistent with the TF threats, vulnerabilities and specificities faced by the jurisdiction, including whether it considers risks identified by other credible sources.

PART 1: GOVERNANCE, SCOPING AND NATIONAL COORDINATION – Good approaches and considerations

Preliminary Scoping and Objective Setting

20. **The objectives of the risk assessment should tie into broader national CTF objectives and activities, and build on existing domestic and regional threat and risk assessments.** The required scope of a TF risk assessment will vary between jurisdictions, but 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. For example, for a jurisdiction that faces a known threat from a specific terrorist group, it may be beneficial to carry out a targeted risk assessment of that specific threat (see textbox 2.2 below on Sweden's targeted TF risk assessment of foreign terrorist fighters). Likewise, where regions share common TF issues, it may be beneficial for jurisdictions to conduct a regional risk or threat assessment, which should feed into the national assessment of risk (see textbox 1.1. below on regional risk assessment initiatives within the Asian Pacific). Alternatively, for a large and decentralized jurisdiction with varying risks within different domestic regions, a series of regional risk assessments may be preferable, or even constitutionally necessary.[22]

21. **In this regard, jurisdiction experience highlights the benefits of carrying out a scoping exercise prior to commencing an assessment of TF risk.** A scoping exercise may consider: potential methodologies and their applicability for the national context, identifying a lead agency or body, and other relevant stakeholders and the availability and gaps of information and data. Textbox 1.2 below describes how the Netherlands drew on both an explanatory study and contextual analysis to identify the desired scope of their 2017 TF risk assessment.

Box 1.1. The Philippines – Regional Scoping and Assessment of TF Risks

Due to common TF threats facing South East Asia (SEA) and Australia, jurisdictions have found benefit in carrying out a number of joint initiatives to assess TF risk at the regional level, which then feeds into national risk assessments. During the Counter-Terrorism Financing (CTF) Summit in Bali in August 2016, members established the Financial Intelligence Consultative Group (FICG), which aims to develop a mechanism for regional financial intelligence analyst exchanges among the ASEAN and close partner FIUs.

Under the auspices of FICG's South East Asian Counter-Terrorism Financing Working Group (SEA CTFWG), relevant jurisdictions conducted a joint study on the different funding methods of ISIL-affiliated groups in the region. The study was divided into four parts: (a) ISIL's Financing in SEA: the Regional Environment (led by the Australian FIU), (b) External Funding

[22] In such cases, federal authorities will need play a coordinating and advisory role to ensure consistent and comparable methodologies and results.

to ISIL SEA (led by the Indonesian FIU), (c) Hawala Dealers Financing of ISIL and Other High Threat Terrorist Organisations in SEA (Malaysian FIU), and (d) Self-Funding of ISIL SEA (led by the Philippines FIU). Participating jurisdictions have found that such regional risk initiatives have served as an effective basis for regional cooperation and have helped to ensure continuity and relevance of assessments.

Box 1.2. Dutch 2017 ML/TF NRA – Explanatory Study and Context Analysis[23]

Prior to commencing their first NRA, the Dutch authorities conducted both an explanatory study and a contextual analysis to gain insight on the methods and data available and applicable, and the unique domestic characteristics that may affect the prevalence for TF. The explanatory study drew on NRA methodologies applied in five countries, additional methods useful for NRAs, and risk valuations that are done (partly in other fields). It concluded that due to the lack of quantitative data, the first NRA should adopt a growth model and should not only analyse the risk of TF, but also identify blind spots, incompleteness and vulnerabilities within the data, TF methods and other information. While the first NRA would focus on the ten most significant TF risks based primarily on qualitative inputs, successive risk assessments may build on these findings with further quantitative inputs. For the context analysis, the Netherlands drew on contextual factors from earlier research and the FATF methodology, and found that the Netherlands' open economy, internationally oriented financial sector, and the scale of criminal income from fraud and drug-related crime may potentially impact the country's vulnerability to TF.

Involvement of All Relevant Competent Authorities

22. **A comprehensive assessment of TF risks will require involvement from a multitude of key authorities, across operational, policy and supervisory functions.** While the specific characteristics of the CT/CFT system differ by jurisdiction (including the mandates, objectives, powers, and formal titles of the key operational authorities), key authorities may typically include: intelligence and security agencies, police and border security (LEAs), prosecution authorities, the financial intelligence unit (FIU), customs, the national authority in charge of implementation of TF targeted financial sanctions, supervisory and regulatory authorities, and foreign counterparts. **In light of the nature the threat, experience highlights the particular importance of involving intelligence and security services when assessing TF risk.** Numerous other competent authorities may hold relevant information, including: tax authorities, social welfare administrations, and

[23] https://english.wodc.nl/onderzoeksdatabase/2689a-verkenning-methoden-en-data-national-risk-assessment-witwassen-en-terrorismefinanciering.aspx

civil aviation authorities (see **Annex B** for examples of relevant authorities based on jurisdiction experience).

23. **Effective national coordination will take different forms depending on the structure of CFT authority and powers domestically**. Experience highlights the particular importance of ensuring high-level commitment (Prime Minister, Government and Parliament) to support the risk assessment process[24], and drawing on existing CFT information-sharing platforms when gathering inputs for the risk assessment (e.g. existing multi-agency task forces, inter-agency centres for strategic threat analysis, shared inter-agency platforms, and suspicious transaction review teams.) Experience also demonstrates the benefits of engaging with key authorities early on in the process (including LEAs and intelligence agencies). The textbox below describes how Belgium's CFT coordination structures generally impacted how they conducted their 2018 TF risk assessment.

Box 1.3. Belgium's 2018 TF NRA – Approach to National Coordination

In Belgium, two separate committees coordinate the fight against ML and TF: the "*Committee Coordinating the Fight against Money of Illicit Origin*" coordinates the fight against ML and the "*National Security Council*" coordinates the fight against TF. Members of the TF committee include: representatives of the federal police, the FIU (CTIF-CFI), civil and military intelligence service, the Customs and Excise Administration, the Federal Public Service (Treasury – responsible for the UN and EU sanction lists), the Federal Prosecutor's Office (in Belgium, the Federal Prosecutor is in charge of the major terrorist and terrorist financing investigations), and the Coordination Unit for Threat Analysis.

As there are two separate coordination committees, Belgium conducted two specific risk assessments: one to assess the ML risks and another one to assess TF risks. Authorities also decided to have two separate coordination committees because of the sensitivity of the information exchanged in the "National Security Council" on terrorism and TF. The CTIF-CFI provided the information sharing mechanism between the ML and the TF coordination Committees.

Engagement with Non-Government Stakeholders – use of multi-stakeholder working groups and public-private collaboration to assess terrorist financing risks

24. **In addition to involving all relevant competent authorities, an assessment of TF risk will require engagement with non-government stakeholders.** Such engagement may include, but is not limited to, the following stakeholders: financial institutions, designated non-financial businesses and professions (DNFBPs), and non-profit organisations (NPOs). **Given that an assessment of TF risk should be an ongoing process, experience highlights the benefits of ongoing engagement and consultation with non-government**

[24] The high-level commitment can also be useful to solve differences in priorities between various competent agencies.

stakeholders, including through relevant supervisors/regulators. Such ongoing engagement also assists to build up trust and open dialogue between relevant parties. Experience also highlights the importance of engagement with a representative sample from the sector (e.g. both small and large entities, and entities from different services etc.), the importance of non-government stakeholder engagement at both the preliminary and validation stages, and clear communication about objectives and purpose of the assessment early on.

25. **Engagement may be facilitated through open or closed online surveys, direct consultation, and the use of existing umbrella organisations, facilitators or interlocutors to encourage dialogue. Countries may also need to carry out multi-stakeholder consultations, as certain sectors may hold vital information for assessing TF risk within other sectors** (e.g. the banking sector will likely hold information relevant for assessing TF risk across a number of sectors). Textboxes 1.4 and 1.5 below describe how both Malaysia and the U.K. have drawn on public-private collaboration to identify and assess TF risk.

Box 1.4. Malaysia – Public-Private Coordination to Assess TF Risk Linked to Designated Persons (Domestic List)

A survey was conducted in 2016 to identify the characteristics of financial transactions performed by all individuals who were designated by the Ministry of Home Affairs (MOHA – Malaysia Domestic List: UNSCR 1373) due to their links to terrorism related activities. The survey involved 20 reporting institutions (including banks, development financial institutions (DFIs) and pilgrims fund board), which were required to conduct analysis on each of the designated person's account held with the institutions for a 24 months review period before their designation. In addition to the assessment on the banking account activities of the designated individuals, the scope was subsequently expanded to include the wire transfer transactions received and conducted by the individuals during the period of 2014 to 2016, to assess any external funding for terrorism activities. Authorities obtained irrelevant information from banks and money services businesses (MSBs) holding licenses for remittance businesses.

Results of both surveys (on banking and remittance transactions) helped identified that: self-funding from legitimate sources is the most commonly used method for raising terrorism funds particularly for travel to or operational use in conflict zones. **Authorities have since used the results to develop the red flags and typologies for TF that authorises have disseminated to reporting institutions in March 2018.**

Box 1.5. The U.K. - Use of Public-Private Partnerships to exchange information on TF risks

The Joint Money Laundering Intelligence Taskforce (JMLIT) was established in 2015 to enable both tactical and strategic intelligence sharing between law enforcement agencies and leading financial

institutions in the UK. The JMLIT brings together law enforcement, the regulator, and over 30 UK and international financial institutions to exchange and analyse information and intelligence. By using the NCA's (National Crime Agency) legal gateway, the JMLIT enables private sector institutions to share information with law enforcement partners and other private sector partners on a multilateral basis. The JMLIT assists in CTF efforts on both the strategic and tactical level.

On the strategic side there is an Experts Working Group (EWG) on CFT. This group is chaired by the National Terrorist Financing Investigation Unit (NTFIU), and the Office for Security and Counter Terrorism in the Home Office (OSCT). It acts as a regular forum (approx. every 6 weeks) at which experts from the public and private sectors can share emerging / newly identified CFT threats and typologies and coordinate project activity designed to combat the threat more effectively. Examples of projects that are currently in process include (not an exhaustive list):

1. Development of typologies on financial indicators associated to home grown / lone wolf terrorists
2. Review of financial indicators common to individuals convicted of CT offences
3. To develop a better understanding of terrorist financing (TF) risks affecting corporate and investment banks (CIB) that can be used to inform CDD / RBA

On the tactical side the JMLIT Ops Group is available to the NTFIU and CT network to support proactive or reactive enquiries into CFT investigations including through an out of hours 'critical incident' function. JMLIT has been utilised on a number of occasions by the NTFIU and has provided a quick and efficient means through which a wide range of tactical information can be requested and obtained. In a number of instances the information provided has proved highly significant to the successful development of the investigation.

Approaches Taken to Overcome Information-Sharing Challenges

26. **Effective inter-agency information sharing is critical to ensure a holistic and credible assessment of TF risks[25].** Nevertheless, the necessary confidential nature of terrorism and TF related information can pose information sharing challenges among competent authorities and with non-government stakeholders when assessing and communicating findings on TF risks. Experience shows the importance of ensuring that jurisdictions have enabling policies and mechanisms that permit information sharing (where possible). Textbox 1.6 below describes how authorities drew on intelligence information in the for the Philippines 2015-16 TF

[25] The FATF RTMG published a confidential report on inter-agency information sharing, including good approaches and practical techniques. This report has been disseminated to relevant competent authorities.

risk assessment. Other good approaches to overcome information sharing challenges when assessing TF risk include:

- Establishing procedures and mechanisms to handle the exchange of sensitive information from an early stage in the risk assessment process (e.g. including engaging with intelligence agencies to ensure relevant safeguards are in place from the beginning of the risk assessment).
- Ensuring that the lead agency is able to access and facilitate the sharing of sensitive information, and where necessary segregating the process of handling sensitive and non-sensitive information (e.g. having a distinct working groups where all participants have appropriate security clearance to exchange information).
- Exploring innovative ways to share information with competent authorities and non-government stakeholders (where possible) (e.g. *through redacted/sanitized reports, extracts of cases, 'closed' briefings, use of anonymized / aggregated statistics; use of proxy organisations/competent authorities to validate information).*

Box 1.6. The Philippines: Use of Intelligence during the 2015-16 TF Risk Assessment[26]

Within the Philippines 2015-2016 national risk assessment, intelligence information from both the FIU (AMLC) and law enforcement/intelligence agencies was used to identify and provide typologies on the source, use, and channels of funds. Intelligence information was shared by the relevant government agencies through focus group discussions. The existing domestic coordination mechanisms (i.e. National Law Enforcement Coordinating Committee and the Joint Terrorist Financing Investigation Group) were tapped in identifying relevant agencies who should participate in the TF risk assessment. All of the identified agencies were already members of these coordination mechanisms, and as such, had a history of and good working relationship. In this manner, agencies were able to share freely information needed to complete the TF risk assessment.

The full version of the report was validated and given to the relevant agencies with appropriate security clearance. A sanitized version of the report was also validated by the participating agencies, and this was published in the AMLC website.

26 www.amlc.gov.ph/images/PDFs/NRAReport20152016.pdf

PART 2: TERRORIST FINANCING RISK METHODOLOGIES – Good Approaches and Considerations

27. **The FATF Standards do not prescribe a particular risk assessment methodology, and there is no one-size fits all approach. Ideally, a risk methodology should be flexible, practical and take into consideration specific features and characteristics of the jurisdiction.** Recognizing that jurisdictions have faced challenges in identifying TF risk to date, the following paragraphs present practical examples of the different approaches that jurisdictions have taken to identify risk. The purpose of this analysis is to highlight the elements of the various TF risk assessment methodologies, including the similarities and differences, rather than to provide a strict formula for how jurisdictions should assess their TF risks.

Information Collection

28. **An assessment of TF risks will require collecting a wide range of quantitative and qualitative information, including on the general criminal environment, TF and terrorism threats, TF vulnerabilities of specific sectors and products, and the jurisdiction's general CFT capacity.** Based on jurisdiction experience, collection techniques may include: gathering of aggregate statistics or information from government sources (whether classified or unclassified), use of domestic and regional questionnaires, online surveys, interviews, working groups and seminars, and gathering open source information. Textbox 2.1 below describes the approach taken by authorities to collect information for the 2016 TF Regional Risk Assessment of South East Asia and Australia.

Box 2.1. 2016 South-East Asia and Australian Regional TF Risk Assessment[27] – Information collection

In 2016 the Indonesian Financial Transaction Reports and Analysis Centre (PPATK) and the Australian Transaction Reports and Analysis Centre (AUSTRAC) co-lead the development of the first Regional Risk Assessment on terrorism financing (RRA TF) for the South-East Asia region, including Australia. The exercise involved collecting inputs from competent authorities of six jurisdictions[28] via a questionnaire and a TF assessment package sent to Financial Intelligence Units. The questionnaire sought inputs on the general TF environment and vulnerabilities in each jurisdiction (e.g. national CFT coordination and cooperation, legislation). The TF risk assessment package collected primarily qualitative inputs on TF threats, vulnerabilities, consequences, including on TF cases. Two regional in-jurisdiction workshops (one in Medan, Indonesia, and one in Manila, Philippines) were conducted to ensure analytical rigour and the accuracy of assessment findings. **Through this process stakeholders identified the benefits of using targeted information collection tools, to prioritise specific questions and enhance the timeliness of responses.**

27 www.austrac.gov.au/sites/default/files/2019-07/regional-risk-assessment-SMALL_0.pdf

28 Australia, Indonesia, Malaysia, Philippines, Singapore and Thailand.

29. The paragraphs below provide some examples of relevant information sources and considerations when identifying TF threats and vulnerabilities based on jurisdiction experience.

TF Threat

30. **Due to the preventative nature of CFT, domestic and foreign intelligence should be a key input when identifying both terrorism and TF threats**. Threat identification should not be limited to perpetrators of terrorist attacks, but more broadly include individuals who travel to conflict areas, as well as individuals and organisations who engage in recruitment, training and facilitation (including fund-raising).

31. **Jurisdictions will need to take a holistic approach when considering terrorism threats, as TF risk may be linked to terrorism occurring in jurisdictions that are not within close proximity**. Jurisdictions will therefore likely need to collect information on domestic and international terrorism threats. When assessing terrorism threat, experience to date highlights that jurisdictions would normally collect information on:

- known domestic terrorist organisations and individuals (including whether nationals are on UN designation lists), known regional and international terrorist organisations or individuals and the extent to which the jurisdiction is a high-priority target for such actors, and information on the nature, ideological motives and the organizational structure of active terrorist organisations;
- volume and location of known terrorist attacks (committed/attempted) domestically or in regional jurisdictions[29];
- domestic or foreign intelligence on global and national terrorism threats[30] (including MLA/extradition requests sent/received, informal requests sent/received);
- parts of the local population which may be sympathetic to active terrorist organisations – *jurisdictions to date have drawn on: information on local population from countries with known active terrorist groups or conflict zones[31], and information from intelligence agencies on terrorism and TF threat within specific communities.*
- intelligence on the volume and characteristics of citizens suspected of travelling overseas for terrorist purposes (i.e. Foreign Terrorist Fighters (FTFs);

---

29 To identify regional terrorist incidents jurisdictions may rely on a range of sources, including outreach to foreign counterparts, and open source information (including the Global Terrorism Database).

30 The FATF has been monitoring evolving TF risks associated with the Islamic State in Iraq and the Levant (ISIL) and its affiliates through regular internal reporting since 2015. The outcomes of these updates may be a useful resource when assessing TF risk, and are accessible via relevant competent authorities.

31 Relevant open sources: World Bank Bilateral Estimates of Migrant Stocks; World Bank Bilateral Remittance Estimates; World Tourism Organisation Statistics.

- expert views from law enforcement agencies, the FIU, and security agencies on the domestic threat of terrorism, and/or;
- open sources information on radicalization amongst domestic populations (e.g. via social media or community engagement).

32. When identifying TF threats specifically, experience to date shows that jurisdictions typically gathered information on:

- funding needs and capacity of known domestic or international terrorist organisations (e.g. level of sophistication), and the extent to which the jurisdiction has communities with links to such groups;
- number and types of known domestic TF cases (including assets frozen pursuant to UNSCRs);
- intelligence on potential domestic TF activity (e.g. STRs, intelligence received from domestic or foreign intelligence agencies);
- intelligence on source, movement and use of funds by citizens suspected of travelling overseas for terrorist purposes (i.e. FTFs);
- financial and trade linkages with countries with active terrorist organisations operating within them and/or conflict zones (e.g. including investment flows) [32];
- volume of active domestic NPOs operating in a conflict zone, and information on known links to terrorist groups or individuals, and/or;
- expert views from law enforcement agencies, the FIU, security agencies, supervisory authorities, and other relevant non-government stakeholders on the level of the domestic TF threat.
- volume of active domestic NPOs operating in a conflict zone, and information on known links to terrorist groups or individuals, and/or;
- expert views from law enforcement agencies, the FIU, security agencies, supervisory authorities, and other relevant non-government stakeholders on the level of the domestic TF threat.

33. **Terrorist organisations and their facilitators are also known to have used similar methods as criminals to raise and move funds and other assets.** Likewise, some terrorist organisations and their facilitators are known to have collaborated with local and regional criminal networks (including smuggling networks) to raise and move funds and other assets in some regions. For this reason, jurisdictions may also need to collect information on the broader illicit finance risks that are not directly related to terrorism (e.g. organized crime profile in relation to specific criminal activities relevant to the jurisdiction). The extent to which such information will need to be collected will depend, in part, on the existence of known links between TF and criminal networks. Textboxes 2.2 and 2.3 below describe

32 Relevant open sources: IMF Consolidated Portfolio Investment Survey, UN Foreign Direct Investment statistics, Central Bank, Statistics Department, World Development Indicators Database.

relevant information sources for Sweden's 2017 targeted TF risk assessment of FTFs, and for the EU's annual Terrorism and Situation Trend Reports.

Box 2.2. Sweden: Targeted TF Risk Assessment of Foreign Terrorist Fighters (FTFs) from Sweden and Denmark during 2013-2016[33]

In 2017 Sweden completed a targeted risk assessment on funding of FTFs from Sweden and Denmark between 2013 and 2016 in order to determine the conditions in place to identify such activities in the future. This targeted study follows on from Sweden's 2015 red flag indicator report. According to the Swedish Security Service, approximately 300 people have travelled to Syria and Iraq since 2012 to join the Islamic State and Jabhat Fatah al-Sham (JFS - previously Jabhat al-Nusra). The general empirical data included a literature review which identified the following indicators linked to FTFs:

- applications for different types of loans (micro loans, SMS loans, student loans);
- applications for credit cards that can be used for cash withdrawal, cash withdrawals in areas bordering the conflict area;
- fund-raising that consists of smaller amounts from many different accounts, unusually high account activity, and;
- purchase of tickets to travel to border zones or trips that pass through the border zone, purchase of pre-paid SIM cards or pre-paid subscriptions for mobile telephones, purchase of outdoor equipment, rental and leasing of specific vehicle models.

Authorities also reviewed the financial activities of Swedish FTFs based on information from public documents, such as preliminary inquiry reports, judgements and fiscal re-examination decisions, as well as information provided by competent authorities (including police, tax authority, secret service, social insurance office, and the economic crime agency.) Thirdly, the study also gathered information about Danish FTFs and similar issues during the same period to identify similarities and differences between the two countries and to identify characteristics of the Danish context that may appear in Sweden.

33 http://fhs.diva-portal.org/smash/get/diva2:1119564/FULLTEXT01.pdf

Box 2.3. EU Terrorism and Situation Trend Reports (TE-SATs) – Information sources[34]

Since 2007 EUROPOL has been releasing an annual public assessment of regional terrorism threats, which draws on inputs from both member states and non-EU countries. The assessment covers jihadist terrorism, as well as ethno-nationalist and separatist terrorism, right and left-wing terrorism, and draws upon information such as: the number of failed, foiled and completed attacks per EU Member State and per affiliation; arrests per EU Member State and per affiliation; convictions and penalties (Eurojust); EUROPOL activities in counter-terrorism; the number of outgoing and returning FTFs; information on use of social media for terrorism purposes; as well as amendments in relevant legislation across EU member states.

Considerations for jurisdictions with no or very few known (or suspected) terrorism or TF cases

34. **It is important that countries assess and continue to monitor their TF risks regardless of the absence of known threats. 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 (including through willing or defrauded donors), 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.

35. Experience shows jurisdictions may rely on techniques such as: scenario building (i.e. likelihood and credibility of common TF typologies for domestic context), and structured interviews and focus groups with domestic or regional operational experts. Textbox 2.4 below describes the approaches taken by Vanuatu and Papua New Guinea (PNG) to assess TF risk in the absence of known TF or terrorism cases.

Box 2.4. Assessing and managing low TF risk - the Papua New Guinea (PNG) and Vanuatu experience

PNG conducted a ML/TF NRA in 2017 that found that the likelihood of TF in PNG is low due to absence of domestic terrorist activity and of communities that might support terrorist activities. However, **there was recognition that this situation could change rapidly and of the**

[34] www.europol.europa.eu/activities-services/main-reports/eu-terrorism-situation-and-trend-report

potentially catastrophic consequences that even a small amount of terrorism funding might allow, necessitate vigilance and a strategy to address TF. The major threat to PNG posed by TF arises from being used as a conduit for the flows of funds intended to fund terrorism noting PNG's geographic location between high TF risk jurisdictions.

Vanuatu conducted a TF risk assessment in 2017 that found no evidence that Vanuatu has been the source of or a conduit for, TF in either the domestic or offshore sectors[35]. **However, there was recognition that the absence of domestic terrorism does not mean that Vanuatu's financial system and institutions cannot be used to raise funds of terrorist activities abroad or to transfer funds form one jurisdiction to another.** This was particularly relevant in light of Vanuatu's role as an Offshore Financial Centre, which presents the opportunity for terrorist financiers to create and employ international companies, legal arrangements and other structures to raise, conceal, move and distribute funds. However, there was no evidence that Vanuatu offshore entities had been used for TF purposes.

In order to test CTF systems despite the identified low risk, both countries adopted comprehensive standard operating procedures (SOPs) and conducted practical training exercises, which provided an opportunity for relevant personnel to apply the legislation and SOPs to hypothetical scenarios. In Vanuatu, a hypothetical desktop exercise was conducted where the legislation and SOP were presented to officers from relevant Government agencies who then worked through a series of hypothetical cases by applying the legislation and SOP to those cases, including stepping through relevant processes and completing relevant forms and templates. It is PNG's intention to run a similar hypothetical desktop exercise for its Government agencies.

TF Vulnerabilities

36. **The assessment of TF vulnerabilities is inherently linked to a jurisdiction's context and identified TF threats.** Textbox 2.5 below describes how Belgium's assessment of TF threats and vulnerabilities were interlinked for their 2018 NRA. Nevertheless, all countries will need to carry out a comprehensive assessment of their TF vulnerabilities regardless of the nature of identified threats, as TF threats may take advantage at any point of loopholes in a jurisdiction's domestic CFT regime. As mentioned above, an assessment of TF vulnerabilities may draw to some extent on known ML vulnerabilities.

37. **Financial and non-financial supervisors as well as the non-government stakeholders will be important participants when assessing TF vulnerabilities, as they can offer a unique perspective on how certain products and services may be exploited**. When considering potential TF vulnerabilities, jurisdiction experience to date highlights that jurisdictions would typically consider:

[35] https://fiu.gov.vu/docs/Vanuatu NRA 2017.pdf

- **Structural elements** (e.g. rule of law, national counter terrorism and TF strategies and activities [e.g. including de-radicalisation/extremism prevention programs], and relationships with regional partners).
- **Materiality** (e.g. extent to which the jurisdiction is a financial or trade hub, relative importance of different parts of the economy, the extent to which the economy is cash based/unregulated, the importance of financial and non-financial sectors which have been highlighted in international typologies as higher risk for TF, as well as cultural links and society demographics etc.).
- **Sector or product-specific TF vulnerabilities**[36] – this should include a consideration of: the extent to which products or services have been misused in known domestic or international typologies, the level of TF awareness and compliance within sectors, and the relative complexity and reach of money movement through sub-sectors or firms that may be higher risk for TF.
- **Compliance with FATF Standards relevant to ML/TF** (e.g. legal framework linked to TF offence and Targeted Financial Sanctions (TFS), preventive measures, cross-border controls, LEA powers and expertise, TF information exchange).
- **Effectiveness of AML/CFT regime and other weaknesses** (e.g. capacity of authorities to identify and prevent TF, effectiveness of TF-related suspicious transaction reporting, monitoring and analysis, quality of intelligence, effectiveness of international CFT cooperation, human resources, and timely access to beneficial ownership information).

Box 2.5. Belgium 2018 National TF Risk Assessment – Relationship between TF threats and vulnerabilities

During Belgium's TF NRA, one of the TF threats identified was the use of cash in the preparation of terrorist attacks. To counter the use of cash Belgium requires strong measures to supervise the (cross-border or domestic) transportation of cash and/or strong measures to limit the use of cash into the economy. The vulnerability assessment therefore looked at the existing measures to reach both objectives and assessed and rated the level of vulnerability of the existing measures.

Another threat identified was the use of social benefit allowances to finance terrorists or a terrorist attack. The vulnerability assessment therefore looked at the existing measures to stop the illicit or unlawful payments of social benefit allowances to Belgian Foreign Terrorist Fighters and identified the vulnerabilities associated with these measures. Notably, the identification of TF vulnerabilities also went beyond the identification of the weaknesses or gaps affecting the sectors subject to AML/CFT measures (reporting entities).

36 Terrorists are also known to have misused public services to raise funds for travelling to participate in terrorist acts, and therefore jurisdictions may also need to consider TF vulnerabilities of public services.

38. Depending on the jurisdiction profile, certain jurisdictions may need to collect further information in order to assess vulnerabilities. The following paragraphs provide some considerations based on jurisdiction experience to date.

Jurisdiction is a global or regional financial or trade centre

39. **Due to the high volume and cross-border nature of assets managed and transferred, international finance and trade centers may be vulnerable to misuse for the movement or management of funds or assets linked to terrorist activity.** In particular, cases have shown terrorist organisations have misused land, sea and air trade to move funds or other assets (e.g. weapons or vehicles) within and between jurisdictions. Common techniques include: under/over-invoicing, or falsification of trade documents[37]. Such activity may be particularly challenging to identify, as terrorist organisations/individuals are known to rely on complex legal structures to hide the underlying beneficial owner.

40. In order to identify potential TF vulnerabilities, good practice to date highlights that financial and trade centers may consider:

- the extent of financial linkages with jurisdictions with active terrorist organisations and/or conflict zones (e.g. data on fund inflows/outflows by jurisdiction, including when available: data on bank deposits, correspondent banking, investments, use of ATMs abroad to withdraw funds from accounts, incoming and outgoing wire transfers, and loads and spends in respect of pre-paid cards);
- the extent of trade linkages with jurisdictions with active terrorist organisations and/or conflict zones, and intelligence and open source information on links between the trade centre and funds or assets (including cargo) linked to designated individuals or entities and their associates;
- the extent to which business relationships and one-off transactions are carried out with parties who are in or are linked to target jurisdictions (including whether financial institutions play an important role as service provider or correspondents for individual customers or FIs located in high-risk jurisdictions for terrorism), and the features and characteristics of those relationships or transactions;
- the extent to which financial or administration services are provided from the financial or trade center in respect of the import or export of goods or other trading activity that could be used for terrorism or to finance terrorist activities;
- the extent to which the financial or trade center is used by foreign PEPs (in light of the possible link with state-sponsored terrorism);
- levels of awareness of TF and trade expertise among the private and public sectors, and ability to detect suspicious behavior;

[37] For relevant cases on trade based TF, refer to: the 2010 FATF study on Free Trade Zones (FTZs); the 2012 Asian Pacific Group Typologies Report on Trade based ML.

- anomalies in available data (e.g. differences in the reported volume of exports from jurisdiction A to jurisdiction B to the volume of reporting imports by jurisdiction B from jurisdiction A).

41. **Assessing TF risk within the trade sector in particular will often require a multi-agency approach with inputs required from customs authorities, the police, the financial intelligence unit, tax authorities, public registrars and intelligence agencies.** Experience highlights the importance of expertise in international trade, as well adequate IT tools to deal with the complexity and large volumes of trade data. Textbox 2.6 below describes a recent initiative by eight European jurisdictions to identify relevant considerations for financial centres with low domestic terrorism risk.

Box 2.6. Monaco (MONEYVAL): Assessing TF Risks for International Financial Centres with low domestic terrorism risk

In April 2018, Monaco held a two-day workshop along with eight other financial centres and TF experts to consider the specific TF risks facing financial centres and the information they could draw on in order to identify, assess and understand these risks. The participants identified ways in which financial centres may be misused for cross-border movement of terrorist funds, including flow-through of terrorism funds, service provision, use of complex structures, abuse of philanthropy, and use of funds generated domestically by illicit activities. Participants also discussed potential information sources to identify financial linkages between financial centres and high-risk countries for terrorism and TF, many of which are presented in this Guidance (refer to paragraph 40 above).

Jurisdiction has a large informal or cash based economy and/or limited state infrastructure

42. **A number of FATF reports have identified use of cash as a common means through which terrorist financiers raise, move and use funds (including through physical transportation via foreign terrorist fighters[38]). Lower capacity jurisdictions with a large cash based economies and informal/unregulated activities can therefore face additional TF vulnerabilities.** When assessing TF risks within the informal sector, experience shows that countries may rely on: findings from credible research studies on the scale and scope of the jurisdiction's informal sector, and information derived from interviews with specific communities. Jurisdictions may also rely on intelligence gathering through other means (including undercover operations), and information on porous borders and identified smuggling networks. For jurisdictions with isolated communities due to limited infrastructure or government presence in some areas, it is vital for competent authorities to engage and seek support from such communities in order to both assess and combat TF risk.

38 See FATFs 2015 Report on Emerging TF Threats.

Country experience highlights that engaging with such communities via a trusted third party may facilitate more open dialogue.

Jurisdiction is within close geographic proximity to an active terrorist threat

43. **Jurisdictions bordering a conflict zone or within close proximity to jurisdictions with active terrorist organisations often face additional cross-border TF threats.** Cases to date have highlighted the use of TF facilitators located in neighbouring jurisdictions to assist in transporting funds and other goods (including foreign terrorist fighters) into or out of conflict zones. For such jurisdictions, an assessment of TF risks will likely include a consideration of the strength of border controls, capacity of customs authorities to identify smuggling linked to TF, and information on the general criminal environment at the border (e.g. presence of smuggling networks). Other relevant factors include: TF awareness and compliance of local financial institutions, DNFBPs or other local sectors vulnerable to misuse, and the extent of engagement and information sharing between domestic and neighbouring authorities.

Box 2.7. Lebanon: 2019 Terrorist Financing Risk Assessment

Lebanon's 2019 ML/TF NRA builds on lessons and experiences gained from the previous 2014 ML/TF NRA. The Special Investigation Commission, Lebanon's FIU led the ML/TF NRA with input from regime stakeholders from the private sector, as well as from the two national committees for AML and CFT.

Backed by high-level political commitment, both qualitative and quantitative data was used for the TF risk assessment part. Vulnerabilities assessed went beyond sectoral and product misuse to examine the contextual framework of the Political, Economic, Social, Technological, Environmental/Geographical & Legislative factors (PESTEL) that ultimately affect an AML/CFT regime. This included a consideration of: related law enforcement resources, the presence of large numbers of refugees with economic/social ties with jurisdictions witnessing terrorism /instability, geographic proximity to the ISIL conflict in neighbouring countries, and having had ISIL and Al-Nusra Front elements entrenched in local mountainous border areas that carried out terrorist attacks in Lebanon.

In order to assess risk including cross-border TF risks, authorities conducted a review of cases handled (suspicious transaction reports, requests of assistance, spontaneous disclosures, TF typologies including NPO misuse). A review of TF convictions revealed that cash was primarily used and that cases of cross-border smuggling did occur. Input from multiple law enforcement agencies and not just customs was used and this covered qualitative as well as quantitative input. This was particularly important, as proximity to an active terrorist threat in neighbouring jurisdictions had necessitated not only having customs, but also other law enforcement authorities including the army monitoring the border to mitigate the risk of illegal border-crossings. Expert opinions from law

enforcement on FTFs that left Lebanon and returnees were also factored in. Cross border TF risks were also identified to arise from terrorist groups' targeting Lebanon from their strong hold abroad, and this at times was made possible by sympathizers and extremists taking refuge or cover within the large refugees communities. TF risk mitigation measures in place were found to be commensurate with the level of risk, with room for some additional measures that were commissioned.

Jurisdiction with strong communal links to active terrorist zones

44. **Terrorist financiers have been known to utilise local diaspora communities, ethnic links and family ties to raise and move funds and other assets to support terrorist activities.** Experience highlights that jurisdictions with strong communal links to areas with an active terrorist threat will typically consider: the potential for sympathetic views to be held by local members of the relevant community (e.g. open source information and intelligence on radicalisation of individuals), and the level of economic activity flowing to and from the local community and regions of active terrorist activity (for example through family support remittances). Jurisdictions may also consider the prevalence of NPOs targeting local ethnic communities for donations to regions with an active terrorist threat.

Analysis of Terrorist Financing Threats and Vulnerabilities

45. **Once jurisdictions have identified known and potential TF threats and vulnerabilities, the next step is to consider how these interact to form risks.** This could include a consideration of how identified domestic or foreign TF threats may take advantage of identified vulnerabilities, based on known cases, or typologies. Some approaches to articulate the interaction of TF threats and vulnerabilities are the use of *hypothetical TF risk events*[39] (see **Annex C**), and/or a combined quantitative and qualitative judgement based on experience.

Sources, channels, direction and use of terrorist funds and other assets

46. **As mentioned above, an assessment of TF risks should include a holistic consideration of all stages of TF: raising, moving, and using funds and other assets. The analysis stage will therefore be likely to involve a consideration of the different sources, channels, destinations and origins of terrorist funds and other assets:**

- **Direction/use of funds** – Fund or other assets might be generated by terrorist financiers in the home jurisdiction, but used by terrorists for operations elsewhere or vice versa. Alternatively, funds or other assets may transit through the jurisdiction for use elsewhere. It is important during the analysis stage that jurisdictions establish the direction and use of terrorism-

[39] TF risk events are hypothetical scenarios derived from a jurisdiction's identified TF threats, vulnerabilities and consequences, which may assist authorities to prioritising between identified risks.

related fund and asset flows, as this information is relevant in determining which controls need to be adopted or strengthened.

- **Sources of terrorist financing** – Sources of financing are likely to differ between different terrorist actors – for example the value and sources of funding for foreign terrorist fighters is likely to differ from the sources used to fund large terrorist organisations. A consideration of the different sources of terrorist financing will enable countries to identify where mitigation controls need to be placed.
- **Channels** – Terrorist financiers use different channels to move funds and assets, including through the banking sector, money service business (MSB) sector, cash smuggling, informal remittances etc. It is important that a jurisdiction's analysis includes a consideration of which channels may be higher risk for TF in order to identify the severity of identified vulnerabilities of specific sectors or products.

Likelihood and consequences

47. **When conducting the analysis stage it is important that jurisdictions prioritise between identified risks. This exercise may involve a consideration of the potential likelihood and consequences of specific TF risks unfolding.** Likelihood and consequence may be assessed or scored using descriptive words or number scales. **The important issue is to use these concepts to differentiate the level of risk presented by diverse types of TF, and thus, assist with prioritising mitigation.**

48. Jurisdictions typically assess likelihood by considering: the prevalence of known cases, intelligence, and typologies, capabilities and intent of terrorist organisations/individuals and supporters, and strength of CFT controls. Given the challenges in calculating consequences, jurisdictions need not take a scientific approach, and instead may want to start with the presumption that the consequences of TF will be severe (whether domestic or elsewhere) and consider whether there are any factors that would alter that conclusion. Textbox 2.8 below describes the approach taken by Argentina to overcome some of these challenges for their 2017-2019 TF NRA. Based on jurisdiction experience, relevant considerations include:

- **Consequences of TF may differ depending on the TF source/channel, or the intended recipient of the funds or assets.** For example, certain channels/sources which enable a high volume of funds to be raised, transferred or used for TF purposes may have higher consequences. However, given the relatively low volume of funds needed to launch a terrorist attack, jurisdictions need to be careful when determining the consequence of TF on the basis of volumes alone.
- **Consequences for many TF risks are likely to be more severe than for ML or other types of financial crime (e.g. tax fraud etc.), which impacts how jurisdictions should respond to identified threats.** By considering the potential consequences of TF this will aid jurisdictions in identifying the appropriate resources to dedicate to combating identified risks and the types of mitigating measures to put into place.

Box 2.8. Argentina's 2017-2019 TF-P NRA – Scoring TF Risks

Argentina is working on a TF Risk Scoring that aims to overcome two of the challenges highlighted above. The AML/CTF National Coordination (NC) has developed two formulas and matrices to score risks associated with **the generation of funds**, and with **the placement, movement, and use of funds,** assessing both the likelihood and the harm/consequences. Due the country has not enough information or evidence of TF cases domestically to score the likelihood of risks, but having much more information at a global level, **the NC has developed the concept of "overall likelihood" that combines a "local incidence sub-score" with a "global prominence sub-score"**. The inclusion of the global incidence sub-score acts as a check against the potential shortcomings of using a likelihood rating based primarily on local authorities' past experience—under-rating the likelihood of risks that may exist but have evaded local authorities' detection, or under-weighting potential emerging risks.

Also considering that the harm/consequences of terrorism and TF risks is always high (wounded and loses of lives and vital infrastructure) and pose challenges to build and work with different levels of risks, **the NC has developed the concept of "marginal harm" (i.e. harm beyond the common base-level of physical harm).** As recent terrorist attacks have demonstrated that the amount of funds raised does not directly correlate to the extent of harm inflicted, the marginal harm score does not include a sub-score related to the amount of funds that can be raised through each method, but instead draws on the FATF's Crime and Terrorism Harm Framework and assesses social, environmental, financial or economic, and institutional or structural harms.

Evaluation

49. **Good approaches to date highlight the particular importance of using qualitative judgment and intelligence sources in reaching conclusions on the relative levels of TF risks in a country.** A common understanding of the relevant levels of TF risk in the country is particularly important in determining how to prioritise mitigation efforts. For countries that face disparate risks within different regions or sectors, it may be necessary to evaluate TF risk at the regional or sector level. **Experience also highlights the benefits of validating findings with different government and non-government stakeholders to avoid confirmation bias and group think, and acknowledging uncertainties or gaps in available information (if applicable).** The textbox below describes Malaysia's approach to evaluating and validating overall TF risks for their 2017 NRA.

Box 2.9. Malaysia's 2017 National TF Risk Assessment – Evaluating TF Risk

Malaysia's third iteration of the National Risk Assessment 2017 (NRA) was completed and endorsed by the National Coordination Committee to Counter Money Laundering (NCC) in July 2018. The assessment drew on a wide range of quantitative and qualitative inputs. During the evaluation stage, subject matter experts were engaged in focus group discussions to provide feedback on the preliminary risk rating, which drew primarily on quantitative inputs (including number of TF cases). These experts comprised of individuals from both public and private sectors, including current and retired law enforcement and government officials, supervisors, regulators, academics, NPOs' representatives, and journalists. Moderation of the risks was also carried out at the National Coordination Committee to Counter Money Laundering (NCC) Working Group level. All members participated in detailed discussions on the preliminary risk rating and compared these against the outcomes from the qualitative assessment to arrive at the final risk rating for each crime.

The proposed final risk rating was then presented to the NCC for further deliberation, consideration and endorsement. Overall, the assessment found that while the inherent risk had increased from medium to medium high since 2013 due to increasing threats posed by the Islamic State (IS) and foreign terrorist fighters in Malaysia and the ASEAN region, such threats had been largely contained by the relevant authorities which had demonstrated considerable capacity to identify and combat TF domestically.

PART 3: ASSESSING CROSS-BORDER AND SECTOR-SPECIFIC TERRORIST FINANCING RISKS

50. **An assessment of TF risk will require a consideration of both cross-border risks and TF risks posed to specific sectors.** The extent to which countries will need to assess the TF risks posed to specific sectors will depend to some extent on the materiality, TF awareness and geographic reach of certain sectors. The below paragraphs present some relevant information sources when assessing cross-border TF risks, TF risks within the banking and Money or Value Transfer Services (MVTS) sectors, and TF risks linked to exploitation of natural resources. These areas have been selected due to their prevalence in international TF typologies; however, the specific areas for increased focus will differ between jurisdictions.

Cross-border Terrorist Financing Risks

Relevant information sources[40]

51. An assessment of cross-border TF risks is typically integrated throughout the assessment of TF risk, rather than being a standalone exercise. Cross-border TF risks may relate to the physical transportation of funds or other assets into or outside a country to support terrorist activities (e.g. cross-border smuggling), the flow of funds, or goods into or out of the jurisdiction via the financial or trade sector, or the cross-border provision of material support (recruitment, training and facilitation).

52. When assessing cross-border TF risks, jurisdictions would typically consult: information on cross-border elements from existing TF information or intelligence, customs/border experience and confiscations, analysis of cross-border declarations/disclosures or cross-border wire transfers (if available), and information on international cooperation related to terrorism and TF. Other relevant sources include: information on inflows/outflows of funds, goods and people, intelligence relating to smuggling networks and the capacity of cross-border controls. Textbox 3.1 below describes the potential use of financial intelligence to assess cross-border TF risks based on jurisdiction experience, and textbox 3.2 below describes Australia's experience in assessing cross-border TF risks.

Box 3.1. Potential Use of Financial Intelligence to Assess Cross-border TF Risks

Cross-border transaction or movement reports (CTRs) – The FATF Standards require that all countries implement a declaration or disclosure system for incoming and outgoing cross-border transportation of currency and bearer negotiable instruments (CBNIs) with a maximum threshold of USD/EUR 15 000 (FATF Recommendation 32.) While the low volume of funds often used by terrorists presents challenges for detection in a threshold-based system, countries to date have found that information on

[40] Notably, chapter 2 above also contains guidance and information sources relevant when assessing cross-border TF risks.

the general inflows/outflows of CBNI may still provide useful information on the potential TF vulnerabilities posed by different borders.

Suspicious Transaction Reports (STRs) – The FATF Standards require that all financial institutions and DNFBPs should be required to notify the FIU if they suspect or have reasonable grounds to suspect that funds are the proceeds of a criminal activity, or are related to TF (FATF Recommendation 20). The value of STRs for strategic analysis purposes is likely to vary between countries depending on the quality and volume of STRs filed. Nevertheless, when assessing cross-border risks, countries to date have found value in analysing STRs for cross-border elements (e.g. suspicious TF funds linked to incoming/outgoing transfer from third country).

Cross-border Wire Transfers (CBWTs) – While not required under the FATF Standards, the collection and strategic analysis Cross-border Wire Transfers (CBWTRs) can prove a useful source of information when assessing TF risk. In particular, countries have found that analysis of CBWTRs at country, sector, and channel levels may provide insights into common destination or conduit countries for transfers, as well as longer-term changes in fund flow patterns. Information on CBWTRs may also be matched with other financial information (such as suspicious transaction reports, or cross-border declarations of cash and bearer negotiable instruments) to identify broader TF patterns and networks.

Box 3.2. Cross-border TF Risk: Lessons Learned from an Australian Perspective

In 2016, the Australian FIU (AUSTRAC) and the Indonesian FIU (PPATK) co-led the Regional TF Risk Assessment (RRA)[41], and in 2017 AUSTRAC co-led a regional study on TF-related cross-border movement of cash and cash smuggling[42]. These studies drew on a wide range of quantitative and qualitative information, including (but not limited to) CT and TF investigations, national security, customs, law enforcement and FIU intelligence, information on international cooperation information, national risk assessments, mutual evaluation reports and industry engagement.

Challenges - Because of the informal nature of some cross-border TF activities (e.g. cash smuggling, hawala etc.), the lack of quantitative data proved difficult. In these instances, details from investigations and intelligence holdings proved most useful. When assessing the risk of TF-related cross-border movement of cash, Australia found that cross-border movement reporting was not particularly helpful it did not capture the key risks, namely self-funding and low-value funding.

41 www.austrac.gov.au/sites/default/files/2019-07/regional-risk-assessment-SMALL_0.pdf

42 www.austrac.gov.au/sites/default/files/2019-06/remittance-corridors-risk-assessment.pdf

Innovative ideas for collection and analysis - To address some of these challenges, AUSTRAC undertook a number of innovative collection and analysis activities, including:

Extensive data-matching exercises including:

(i) **Matching arrested persons and persons of interest (POI) lists to financial transactions.** These results highlighted POI touchpoints with reporting entities, and could identify which financial sectors, products, services and delivery channels POIs may have be using;

(ii) **Matching immigration data with Threshold Transaction Reports (cash transactions valued at AUD 10,000 or more) and Cross-Border Movement of cash reports**. This identified individuals who had entered Australia, made a large cash deposit, but who failed to submit a Cross-Border Movement of cash with border authorities;

(iii) **Matching Cross-Border Movement of cash customers to SMR customers.** This could identify entities who had legitimately declared their cash upon entry to Australia, and had previously been identified reporting entities for suspicious behaviour or financial transactions.

Leveraging partner agency covert investigation powers to proactively collect intelligence, and leveraging Customs and Border authorities to conduct operations to detect undeclared Cross-Border Movement of cash.

Labelling partner agency investigations and Intelligence Reports[43]. AUSTRAC designed a labelling app to record a wide range of details relevant to TF threat and vulnerabilities.

Labelling AUSTRAC Intelligence Reports[44]. AUSTRAC designed a labelling app to record a wide range of details relevant to TF threat and vulnerabilities.

Creating a dynamic matrix to measure threat. This matrix allowed the assessor to assign a quantitative risk rating, even when primarily qualitative data inputs were used. AUSTRAC found this type of rating system resonated with industry stakeholders and removed ambiguity in the rating process.

Engaging with foreign counterparts

53. **Experience shows that ongoing engagement with foreign counterparts is particularly important in both detecting and assessing cross-border TF risks.** Experience highlights the benefits of establishing regular contact points for terrorism and TF-related information exchange, formal analyst exchanges and the co-location of personnel. The textboxes below describe: (i) a joint initiative by the Philippines, Malaysia, Indonesia and Australia to understand the cross-border flow of funds, fighters, and material support to the MAUTE Group and associated groups; and (ii) a

43 This app allows a quantitative measure of qualitative data.
44 This app allows a quantitative measure of qualitative data.

joint analysis exercise conducted within the European Union (EU) FIU platform to identify TF risks.

Box 3.3. The Philippines, Malaysia, Indonesia, and Australia: 2018 Analyst Exchange Program (AEP)

The 2018 Analyst Exchange Program (AEP) was a multi-lateral project involving financial intelligence analysts from the Australian Transaction Reports and Analysis Centre (AUSTRAC), Pusat Pelaporan Dan Analisis Transaksi Keuangan (PPATK), Anti-Money Laundering Council (AMLC), and Bank Negara Malaysia (BNM). The aim of the Program was to identify and understand the flow of funds, fighters, and material support to the MAUTE Group and associated groups in the Philippines prior to and during the Marawi Seige in 2017. The AEP participants were able to identify money moving networks, probable fund sources, networks used, and previously unknown financiers and facilitators being utilised to finance terrorist groups in the Southern Philippines. The findings were circulated to regional LEAs, and have supported ongoing investigations. At every stage in the process, AEP participants briefed their domestic LEAs and other partner agencies for the purposes of validating the AEP findings. During the meetings, participants shared information on: Financial Intelligence Reports (FIRs) / summary reports generated by FIUs, various transaction reports, various information/intelligence from the domestic authorities such as travel / immigration records, company registration records, customs records, police and military intelligence, financial intelligence / information provided by entities from the private sector (including information not previously reported through regular transaction reporting regimes).

Box 3.4. Italy's TF Risk Assessment – Contributions from the Joint Analysis of TF Cases Within the European Union FIUs' Platform

Within the European Union (EU) FIUs' Platform, the Italian FIU (UIF) in 2017 promoted and coordinated a joint analysis of TF cases that had a multi-jurisdictional dimension. This exercise aimed at pursuing complex TF cases that an individual FIU could not easily detect in isolation. Through this exercise, a new method for joint analysis was developed which fostered the joint consideration of cases by teams of FIU analysts involved (i.e. the FIUs of the Netherlands (co-lead, as well as FIU Italy), Belgium, France and Spain). The projects were successfully finalised in meetings hosted by UIF in November 2018 and were subsequently endorsed by the EU FIUs' Platform. Apart from the material findings related to the specific cases analysed by the teams, these projects provided knowledge and expertise that proved useful for the Italian National Risk Assessment:

- on the one hand, the projects offered confirmation of techniques and operational schemes regularly seen in TF STRs (e.g. network analysis and pattern recognition), and;
- on the other hand, the experience of sharing the financial analysis with FIUs' of nearby countries naturally focussed the operational efforts on the cross-border dimension, thus improving the analysts' expertise in qualitatively assessing TF risks from this fundamental perspective.

Sector-specific Terrorist Financing Risks

54. When assessing the TF risks facing a specific sector, experience shows that the relevant supervisors as well as the sector itself will be important stakeholders.

Banking sector

55. **As noted in the 2015 FATF Report on Emerging Terrorist Financing Risks[45], the banking sector is an attractive means for terrorist organisations seeking to move funds globally because of the speed and ease at which they can move funds internationally**. The low value of funds often used by terrorist financiers, and the sheer size and scope of financial flows gives terrorist organisations and their financiers the opportunity to blend in with normal financial activity. Importantly, for many jurisdictions, the banking sector is subject to the most robust AML/CFT requirements (relative to other financial institutions)[46]. When assessing TF risk facing the banking sector, jurisdictions would typically collect information on: the types of banking institutions and the lines of businesses or services offered, the types of customers served by banks, the nature of TF threats posed to the sector, as well as AML/CFT compliance and awareness within the sector. Textbox 3.5 below provides more detailed examples of relevant information which competent authorities would typically consider based on jurisdiction experience.

Box 3.5. Potential Considerations When Assessing TF Risk in the Banking Sector Based on Jurisdiction Experience

- **The TF threat posed to the sector:** information on how terrorist organisations or individual terrorists accessed or misused the banking system in the jurisdiction, and open source information concerning links

45 www.fatf-gafi.org/media/fatf/documents/reports/Emerging-Terrorist-Financing-Risks.pdf

46 FATFs 2014 Guidance for a Risk Based Approach (RBA) for the Banking Sector provides additional information relevant to assessing and mitigating TF risk within the sector in line with a RBA: www.fatf-gafi.org/media/fatf/documents/reports/Risk-Based-Approach-Banking-Sector.pdf

between domestic banking institutions and foreign legal or natural person (including financial institutions) with links to TF[47].

- **Types of banking institutions and lines of business or products/services offered**: information on the materiality of the sector, including the types of services are offered (retail services, wealth management, corporate/commercial banking, or correspondent banking), and the volume and location of branches. Certain factors may make different services vulnerable to TF. For example, past FATF reports have identified the use of pre-paid cards for TF purposes[48]. Likewise, retail banking services that allow for person-to-person funds transfers can be vulnerable to misuse by terrorist supporters seeking to quickly move funds overseas, while banks providing correspondent services (particularly nested accounts) may lack full information about the ultimate originator and beneficiary of cross-border funds transfers.
- **Customers Served by Banks**: jurisdictions should also consider whether certain types of corporate or individual customers may be more closely associated with TF. This could include corporate customers who are identified for being at a higher-risk for TF, as well as individual customers who are identified, through the use of contextual information, as potentially being associated with terrorism or TF.
- **AML/CFT Compliance within the sector**: While any deficiency in a jurisdiction's AML/CFT legal framework can pose a potential vulnerability, weaknesses in the following areas may be more closely tied to TF vulnerabilities for banks: *STR filing requirements for TF (no filing requirement or a low number of filings); no authority or ability to share information with the private sector; and weak implementation of (i) targeted financial sanctions or (ii) customer due diligence obligations or internal controls (especially for clients in high risk areas or lines of business).*

Money Value Transfer Services (MTVS)/Remittance sector

56. **As noted in the 2008 FATF Typologies Report on Terrorist Financing[49] and the 2015 Emerging Terrorist Financing Risks report, the MVTS/remittance sector has been exploited to move illicit funds and is vulnerable to TF.** In conflict-affected jurisdictions where access to banking services is limited and terrorist organisations operate, remittance providers may be the primary financial institution

47 Some jurisdictions have found that supporters associated with certain terrorist organisations more frequently used the banking system to transfer funds than other terrorist organisations.

48 www.fatf-gafi.org/media/fatf/documents/reports/Emerging-Terrorist-Financing-Risks.pdf

49 www.fatf-gafi.org/media/fatf/documents/reports/FATF%20Terrorist%20Financing%20Typologies%20Report.pdf

through which consumers can engage in cross-border funds transfer activity. Moreover, the cash-intensive and informal nature of some remittance services can expose such entities to TF risks.

57. **When assessing the TF risks within the MVTS/remittances sector, jurisdictions would typically consult information on the nature of the sector and services offered (i.e. prevalence of services which favour anonymity), the scope of unregulated actors, the nature of TF threat, and AML/CTF compliance and awareness within the sector.** Experience also highlights that engagement with diaspora communities is important in order to identify how such communities transfer money into, or out of, the jurisdiction. This is particularly the case for local or foreign populations that may be more sympathetic to foreign terrorist organisations and actors. Textbox 3.6 below provides more detailed examples of relevant information which competent authorities would typically consider based on jurisdiction experience.

Box 3.6. Potential Considerations When Assessing TF Risk in the MVTS/Remittance Sector Based on Country Experience

- **TF threat posed to sector:** Are there local diaspora populations that may be sympathetic to regional or international terrorist actors? How do such communities transfer money abroad? How have terrorist organisations or terrorists accessed or misused MVTS/remittance providers domestically and/or in common international typologies?
- **Types of MVTS/remitters and lines of business, products or services offered:** the size and scope of MVTS sector (i.e. small remitters that deal directly with their customers or large-scale MVTS providers operating through established banks?);the scale of services offered that favour anonymity for sender or receiver, including non-face-to-face interactions, and/or facilitate quick cross-border transfers; and the scope of unlicensed MVTS providers operating domestically.
- **Customers Served by MVTS/Remitters[50]:** The following characteristics may indicate a higher vulnerability for TF: transactions indicating that a customer operates a cash-based business that appears to be a front or shell company or is intermingling illicit and licit proceeds, a customer knows little or is reluctant to disclose details about the payee (address/contact info, etc.), or a customer is involved in the transactions that have no apparent ties to the destination country and with no reasonable explanations.
- **Agents:** What share of remitters in the jurisdiction rely on agents or other third parties to undertake customer due diligence? If agents are commonly used, what type of relationship do they have with the remitters? Are agents subject to regulation and supervision, and what fit and proper checks do they undergo?

50 Jurisdictions should also consider whether a segment of their MVTS providers serve corridors that include jurisdictions or areas identified as providing funding or support for terrorist activities or that have designated terrorist organisations operating within them.

- **AML/CFT Compliance:** Weaknesses in the following areas may be more closely tied to TF vulnerabilities: *STR filing requirements for TF (no filing requirement or a low number of filings); no authority or ability to share information with the private sector; and weak implementation of (i) targeted financial sanctions or (ii) customer due diligence obligations or internal controls (especially for clients in high risk areas or lines of weak onsite supervision or enforcement).* Additionally, if MVTS providers are not subject to licensing or registration, that would constitute an important vulnerability.

Unregulated MVTS Providers and Hawala[51]

58. **While limited banking access in some jurisdictions leads legitimate customers to use unregulated MVTS, there are multiple examples of terrorists and their financiers using Hawala or other similar service providers (HOSSPs) to transfer funds[52].** In addition to assessing their regulated MVTS/Remittance sector, jurisdictions should also attempt to assess the scale of activity undertaken by unregulated or unlicensed MVTS providers. In considering this vulnerability, jurisdictions should consider: actions taken to identify and sanction unregulated MVTS providers and, and the country's compliance with FATF Recommendation 14[53]. **Notably, the identification of unregulated actors will typically involve engagement with regulated MVTS**. Other relevant sources of information may include: bilateral remittance data, and the role of informal remittances in TF investigations and STRs.

59. **Jurisdictions may need to develop better coordination between regulators and law enforcement in order to proactively identify and try to bring within the formal sector those who operate MVTS illegally.** Lack of clarity regarding which agencies are responsible for taking the lead on dealing with illegal unlicensed or regulated MVTS can be a substantial AML/CFT vulnerability.

Other Terrorist Financing Risks

Exploitation of natural/environmental resources

60. **Terrorist organisations such as ISIL, al-Shabaab and al-Qaeda have relied on natural resources in their area of control (oil, gold, charcoal, talc, lapis-lazuli, etc.) as a source of income.** Supply chains in source, transit and end-use jurisdictions may be vulnerable to exploitation. Countries that are rich in natural/environmental resources, and particularity those with active terrorist organisations operating, will need to consider the TF risks associated with exploitation of such resources. In doing so, jurisdictions would typically consider (among other information): the transport routes and locations of extraction, trade,

51 See, FATF Guidance for a Risk-Based Approach: Money or Value Transfer Services (2016) for further information.

52 FATF Report on the Role of Hawala and other similar service providers in money laundering and terrorist financing (2013), page 41.

53 FATF Recommendation 14 requires countries to take action, with a view to identifying natural or legal persons that carry out MVTS without a licence or registration, and applying proportionate and dissuasive sanctions to them.

handling and export of the natural resources, and the strength of regulations for dealers in precious metals and stones. Textbox 3.7 below provides more detailed examples of relevant information which competent authorities would typically consider based on jurisdiction experience.

Box 3.7. Potential Considerations When Assessing TF Risk Linked to Exploitation of Natural/Environmental Resources

- **Involvement in the extraction of natural resources[54]:** Are there terrorist organisations operating in or controlling territory in the jurisdiction in areas rich in natural resources? It may be useful to overlay key extraction/collection/mining sites with maps depicting areas of activity by terrorist organisations to identify potential vulnerabilities.
- **Extortion:** What are the transport routes and locations of extraction, trade, handling and export of the natural resources? Have there been reports of terrorist organisations being active in these areas? It may be worthwhile engaging with the private sector (mining or oil companies, logistics and security services providers) to understand what their transportation networks are impacted.
- **Variations in imports/exports[55]:** Trade data may be useful in identifying variations in the import or export of natural resources. For example, a drop in the export of gold in one jurisdiction and sudden increase in the export of gold in a neighbouring jurisdiction could be an indicator that resources are being moved to a neighbouring jurisdiction to avoid domestic controls. Similarly, reconciling import and export data with another jurisdiction's data could highlight discrepancies.
- **Exposure of transit or end-user jurisdictions:** To what extent are natural resources imported from higher-risk jurisdictions? Some jurisdictions function as transit hubs particularly for precious stones and metals brought in through cabin luggage. What are the numbers of undeclared natural resource imports? What measures exist to detect smuggled precious metals and stones, at airports, for example? What due diligence measures are undertaken on supply chains and sourcing decisions?
- **Movement of funds:** Are terrorist organisations using precious metals or stones, or other resources to bypass the official banking system? Are there weaknesses in the regulation and supervision of dealers in precious metals and stones?

54 Ministries of mines, trade or environment, as well as LEAs and intelligence agencies, industry associations and civil society groups may have relevant data.

55 The OECD's assessment of gold supply chains in Burkina Faso, Mali and Niger also highlights how engagement with local stakeholders and analysis of trade data may provide indications of TF risks: http://mneguidelines.oecd.org/Assessment-of-the-supply-chains-of-gold-produced-in-Burkina-Faso-Mali-Niger.pdf

PART 4: NON-PROFIT ORGANISATIONS AND ASSESSING TERRORIST FINANCING RISK

61. **Recognising the requirements under Recommendation 8 (R.8) to assess TF risks facing those NPOs that fall within the FATF definition, this chapter provides some considerations and good approaches based on jurisdiction experience**. The general guidance provided in other parts of this report is also relevant for the assessment of TF risks associated with NPOs. Of particular relevance are the general issues relating to national coordination and stakeholder engagement (included in chapter 1), and the need to maintaining an up-to-date understanding of risk (dealt with in the chapter 5 of this report).

62. **In June 2016, the FATF revised R.8 to ensure its implementation is in line with the risk-based approach and does not disrupt or discourage legitimate non-profit activities**[56]**.** The revisions clarified that not all NPOs represent the same level of TF risk, and that some NPOs represent little or no risk at all. Experience shows that jurisdictions continue to face challenges in assessing TF risk in this area due in part to: the large and often diverse nature of the sector, a lack of identification or understanding of those NPOs falling within the FATF definition, and the limited availability of relevant quantitative information or cases.

FATF Requirements on Identifying and Assessing TF Risk Facing NPOs

63. FATF R.8 provides the requirement to assess risk facing NPOs, and is focused specifically on TF. R.8 requires jurisdictions **to undertake a domestic review of their NPO sector**, or have the capacity to obtain timely information on its activities, size and other relevant features, **in order to identify the subset of NPOs that fall into the FATF definition**. In doing so, jurisdictions are required to use all available sources of information **in order to identify features and types of NPOs that, by virtue of their activities or characteristics, are at risk of being misused for TF**.

FATF defines an NPO as: "*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'.*" This functional definition is based on those **activities** and **characteristics** of an organization **that puts it at risk of TF**, rather than on the simple fact that it is operating on a non-profit basis.

[56] These amendments were informed by the June 2014 FATF Report on Risk of Terrorist Abuse in NPOs and the 2015 FATF Best Practices Paper on Combating the Abuse of NPOs.

Figure 4.1. Recommendation 8 Figure

The below figures provides an example of a jurisdiction's NPO sector. The volume of NPOs which fall within the FATF definition will vary between countries.

64. When assessing risk, **R.8 requires jurisdictions to identify the nature of threats posed by terrorist organisations to NPOs deemed to be at risk as well as how terrorist actors abuse those NPOs.** Similarly, jurisdictions should **review the adequacy of measures, including laws and regulations, which relate to the subset of the NPO sector that may be abused for TF** in order to be able to take proportionate and effective actions to address identified risks. The FATF Standards highlight that the review should go beyond laws and regulations, and that existing measures may already sufficiently address identified risks. R.8 requires jurisdictions to **periodically reassess the NPO sector** by reviewing new information on the sector's TF vulnerabilities.

Examples of Considerations and Good Approaches

65. Recognizing that the FATF Standards do not prescribe a particular method or format for assessing risk, the following paragraphs provide some good approaches based on jurisdiction experience in assessing TF risks facing NPOs. **Annex D** provides examples of potential information sources to support the identification and assessment of TF risks among those NPOs that fall within the FATF definition.

Understanding the sector

66. **A comprehensive understanding of the features, nature and activities of the sector is a vital pre-requisite to understanding the TF risks posed to some NPOs.** A domestic review is a key component of R.8 and is a critical starting point for assessing TF risk by determining which NPOs fall within the FATF definition. **Importantly, the FATF definition of NPOs may not be synonymous with national definitions or legislation for NPOs, as the definition is primarily functional (i.e. defines NPOs by their activities), and in many jurisdictions NPOs are classified**

by their legal form (e.g. association, charities etc.). In addition, there may be entities which meet the FATF definition of an NPO which do not fall within national NPO legislation.

67. A jurisdiction's domestic sector review could include information on: the types of organisation(s) and the purpose(s) for which they were established, the location of activities in which they are engaged, the services provided, their donor base, the value of sector assets, movement of funds, means of payments, and the cash intensity of the sector.

68. In identifying the types and features of NPOs that may be vulnerable to TF misuse, jurisdictions may also want to consider: domestic and foreign intelligence on misuse of NPOs, investigations and suspicious activity, domestic or international TF typologies related to NPOs and inputs from civil society representatives (including sector or organisational self-risk assessments). This exercise will likely involve a consideration of both the sectoral and organisational vulnerabilities[57]. The below textboxes describe the approaches taken by Malaysia, and the U.K. when conducting their domestic reviews.

Box 4.1. Malaysia 2017 NPO Risk Assessment

Separate from its ML/TF NRA, Malaysia carried out a TF risk assessment of those NPOs that fall within the FATF definition in 2017.

The first part **involved a comprehensive domestic review of NPO sector's landscape in Malaysia**, which included understanding the overall NPO population, distribution of services and expressive NPOs, value of NPO assets, and the movement of NPO funds. This domestic review also included an overall assessment of the legal and regulatory regime for administration of NPOs to identify those that fell within the FATF definition.

The second part was the assessment of **TF risks in relation to NPOs**, specifically aimed to identify inherent TF risks facing NPOs identified as vulnerable to TF and the control measures in place to mitigate identified risks. The analysis of the findings was then subject to validation, involving 31 regulators, LEAs, NPOs and academics, to ensure the robustness of the assessment, before the findings were finalised for deliberation and adoption by the National Coordination Committee to Counter Money Laundering (NCC).

57 Sectoral vulnerabilities may include: vulnerabilities in the registration process (i.e. sham charity enters the NPO sector), while organisational vulnerabilities may include weak internal controls, financial management and planning (i.e. funds from individual NPO may be diverted for terrorist individual/group.)

Box 4.2. U.K: 2017 Domestic Review of NPO sector

The U.K.'s Domestic Sector Review of its NPO sector (2017), had three primary components:

Identifying and examining the size, scope, and composition of the entire NPO sector in the U.K. Data from published reports on the U.K.'s NPO sector was augmented with information requested from various government departments and agencies with responsibility for registering/regulating NPOs.

Evaluating NPO structures and oversight: To understand the legal structures and reporting requirements of organisations within the U.K. NPO sector, the review determined what information each regulatory body/agency collected to help assess levels of transparency and oversight.

Identifying the subset of NPOs that operate in the U.K., that fall within the FATF definition, which may be at the greatest risk of terrorist financing abuse and therefore subject to Recommendation 8. The analysis took into account the findings of the FATF report Risk of Terrorist Abuse in Non-Profit Organisations ('the Typologies Report') and the U.K.'s 2015 National Risk Assessment ('NRA'). Consideration was also given to the work across government as part of the U.K's second NRA which was ongoing at the same time. The 2017 domestic review considered recent case studies of TF involving NPOs, the stated purposes of relevant NPOs, areas of operation and geographical location in the U.K. In addition, the review conducted a trend analysis of historic cases.

Regulators and government departments with responsibility for regulating/overseeing the activities of the NPOs – separate from those registered or regulated by the U.K.'s charity regulators – were approached via a survey enquiring about the NPOs under their purview. The survey responses provided information about investigations or any evidence or allegations of NPO TF abuse. Enquiries were also made with relevant law enforcement agencies. A review of published studies and other materials both by the NPO sector itself and others relating to its composition were also considered.

Identifying the nature and threat posed by terrorist organisations to NPOs deemed to be at risk

69. **When assessing the TF threats facing those NPOs identified as vulnerable to TF misuse, jurisdictions will typically consider:** the general terrorism and TF threat environment, prevalence of domestic intelligence on the TF threat posed to NPOs, existing regional and international typologies (and their applicability for the domestic context), and credible open source information on links between domestic NPOs and terrorist individuals or organisations. For general considerations when identifying TF and terrorism threats, see chapter 2 above.

Reviewing the adequacy of measures, including laws and regulations

70. **When reviewing the adequacy of measures which relate to NPOs that are assessed as being more at risk of being misused for TF, jurisdictions may also consider:** self-regulatory governance and transparency measures (at the sector and organisational level), policy measures by government (including outreach to the sector), and national CFT capacity more generally. Textbox 4.3 below describes the approach taken by the U.K. for this exercise.

Box 4.3. U.K.: Review of Adequacy of Measures Including Laws and Regulations

When reviewing the adequacy of measures that apply to those NPOs identified as vulnerable to TF, the U.K. considered the relevant legislation and regulations, as well as self-regulatory measures and the adequacy of relevant outreach and guidance to the sector.

Following a review generated by the Charity Commission of England and Wales (CCEW) in 2014/15, the Charities Act 2011 was amended in 2016, to enhance or introduce a number of powers available to the CCEW and included a provision which expands the automatic disqualification of certain individuals from holding the position of charity trustee – this includes those individuals who are convicted of terrorism offences, as well as individuals subject to financial sanctions. This was as a result of identified gaps and deficiencies in the CCEW's legislation at that time to address abuse and wrongdoing of the charity sector in England and Wales including abuse for terrorist purposes. Section 16 of the Charities Act 2016 mandates that a review is conducted within three years of the Charities Act, 2016 coming into effect and that a report of the review is published within four years.

Competent authorities also actively seek feedback on the adequacy and relevance of its published guidance, and in 2018 conducted a survey of charities operating internationally (those that were identified as the subset of higher risk NPOs) to obtain feedback on its guidance, where improvements could be made to the resources and tools available for trustees.

Engaging relevant competent authorities, the NPO sector and other non-government stakeholders

71. National coordination can pose particular challenges for conducting a risk assessment of NPOs, as relevant information is often spread across a number of ministries and agencies. **Government agencies that have oversight over a part of the NPO sector (including regulators/supervisors, or self-regulatory bodies) will need to play a central role when assessing TF risk.** In addition, experience shows jurisdictions would typically also consult:

- **Tax authorities –** in many jurisdictions, NPOs subject to tax exemptions are required to file annual financial statements and statements of purpose with

the tax authorities, and such agencies may be able to provide important contextual information on NPOs. **Importantly, R.8 does not require jurisdictions to consider NPOs as reporting entities.**

- **Financial intelligence Unit (FIU) –** FIUs may be able to provide valuable financial intelligence to assist in identifying TF risks posed to NPOs, either through access to suspicious transaction reports, or wire transfers, and/or information on common typologies and trends for TF.
- **Law Enforcement Agencies (including customs authorities)** – LEAs are an important source of information on the general threat profile for terrorism and TF and the criminal environment facing those NPOs identified as vulnerable to TF.
- **Intelligence Agencies** – Intelligence authorities will also be an important source of information on the terrorism and TF threat environment, including information received from foreign counterparts. For good approaches in overcoming information sharing challenges related to confidentiality, refer to Chapter 1 above.

72. The case study below from Australia illustrates how, when developing Australia's 2017 National NPO risk assessment, information was sought from a wide range of commonwealth, state and territory public sector agencies, financial, criminal and national security agencies, and representatives from the NPO sector.

Box 4.4. Australia's 2017 National NPO Risk Assessment Approach: Data collection and stakeholder engagement[58]

When developing Australia's 2017 National NPO risk assessment, the collection of information was divided into two stages: the first involved identification and collection of existing documents and other relevant data holdings. This included open source documents, as well as classified data, financial intelligence and details of criminal/national security investigations. Australia's FIU (AUSTRAC) led the collation of a NPO high-risk dataset (which was later analysed to identify key risk indicators) comprised of 28 Suspicious Matter Reports (SMRs), case studies, investigations and intelligence holdings. During this phase, Australian Charities and Not-for Profits Commission (ACNC) and (Australian Tax Organisation (ATO) also led a review of current regulatory landscapes to identify sector vulnerabilities in existing laws, reporting requirements and governance.

The second part involved stakeholder engagement. A formal request for information was sent to 23 agencies including all Commonwealth, state and territory law enforcement bodies and NPO regulators. The ACNC and AUSTRAC convened round-table meetings with NPO members and peak body representatives to gather sector insights regarding the nature and extent of TF misuse of the sector. During this phase, AUSTRAC and ACNC also developed and distributed a TF risks perceptions survey. The survey

58 www.austrac.gov.au/sites/default/files/npo-risk-assessment-FINAL-web.pdf

gathered views from government, industry, NPO peak bodies and experts to understand the scale of concerns regarding the nature and extent of NPO abuse for TF (threat), sector and organisational vulnerabilities, and develop key findings regarding overall risk. AUSTRAC was able to use some of the quantitative data to undertake unique data-match activities to help identify higher-risk NPOs (e.g. matching the list of NPO names against national security intelligence holdings).

To ensure the accuracy of the risk assessment findings, the assessment was developed in consultation with members of the NPO sector. This included providing the final risk ratings for review. Structured consultations were also held with key government stakeholders and terrorism financing experts to collect information, capture a wide range of intelligence, policy and supervisory perspectives, and evaluate findings and judgements.

73. **Ongoing engagement with the NPO sector is important in the success of any efforts to identify and assess TF risks within the sector and was identified by NPO representatives as a critical component for them**. Engagement and outreach with the NPO sector is also a key element of FATF R.8 that requires jurisdictions to undertake outreach to the NPO sector concerning TF issues. For the NPO sector, where there may be a lack of prior engagement, jurisdictions should consider outreach via trusted representatives, and should ensure engagement with a representative sample (e.g. umbrella organisations and service NPOs.) Experience also highlights the use of open online surveys and questionnaires as a good approach to ensure broader feedback from NPOs. Textbox 4.5 and 4.6 below describe how both Kosovo and Kyrgyzstan sought inputs from NPOs during their risk assessments.

Box 4.5. Kosovo's[59] 2017 Sector Specific Risk Assessment on Terrorism Financing in the NPO Sector

Given the particular perceived sensitivities with the engagement of NPOs in a government information gathering exercise the Working Group decided that another NPO would be engaged as an 'agent' to carry out face-to-face interviews with a selected cross section of NPOs and assist them in completing the questionnaire. The 'agent' compiled a list of a 150 NPOs in Kosovo and this list was agreed by the Working Group. The compiled list of NPOs that was given to the Working Group was entirely based on the official list received from the Ministry of Public Administration and the lists from Kosovo's municipalities for all the active NPOs in their regions. In order to build in resilience (in the event that a selected NPO refused to engage in the process) a further 21 organisations were placed onto the list. Ultimately, the 'agent' was able to interview a total of 150 NPO, from a cross- section of organisation types. Moreover, Kosovo Islamic Society (BIK) was a strong contributor to the risk assessment working group.

[59] This designation is without prejudice to positions on status, and is in line with United Nations Security Council Resolution 1244/99 and the Advisory Opinion of the International Court of Justice on Kosovo's declaration of independence.

74. In addition to the NPO sector, it may also be helpful for jurisdictions to engage with financial institutions who may be able to provide valuable information on the types and nature of transactions related to NPO clients. Additionally, it is beneficial that jurisdictions engage with financial institutions to ensure that they effectively understand the TF risk to their NPO customers and that the possibility of unsubstantiated de risking is reduced.

Box 4.6. Kyrgyzstan – NPO Engagement During the TF Risk Assessment

During the first half of 2019, NPOs in Kyrgyzstan have been included in the government-led working group on conducting the NPO sector risk assessment. The FIU issued a public call for civil society representatives to become formal members of the risk assessment working group, with three NPOs appointed to the group. NPO representatives worked with government to identify and adapt a methodology developed by an international consultancy for use in Kyrgyzstan. This methodology requires active engagement of the NPO sector, to increase accuracy of the data collected, increase awareness about the potential risks and protective measures, build trust among the sectors and enhance buy-in for the recommendations and results.

PART 5: FOLLOW UP AND MAINTAINING AN UP-TO-DATE ASSESSMENT OF TERRORIST FINANCING RISKS

75. **Jurisdictions should ensure that the findings of the TF risk assessment are endorsed by senior officials, and that all key stakeholders have a common understanding of the outcomes and the relative measures of risk (i.e. "low" or "high" across different types of TF risk, and/or compared to other domestic crimes).** The FATF Standards require that jurisdictions have a mechanism to ensure that competent authorities and respective financial institutions, DNFBPs and other relevant sectors are aware of the results of national TF risk assessment(s). Given the sensitive nature of terrorism and TF-related information, experience highlights the particular benefits of disseminating a sanitized version of the report, and holding closed briefings with key stakeholders to ensure there is a common understanding of the outcomes.

76. **An assessment of TF risk should result in clear and practical follow-up actions.** Such follow-up actions may include (but are not limited to): amendments in CFT legislation and policies to address identified deficiencies, allocation of resources or training to key authorities, development of platforms or mechanisms to enhance information sharing on TF, enhanced engagement with sectors or institutions identified as vulnerable to TF, and/or implementation of a more systemic mechanism for collecting and maintaining TF or terrorism related information. Experience to date highlights the importance of clearly allocating and codifying (if possible) which authorities are responsible for follow-up actions (including updating the risk assessment), as well as setting timelines.

77. **The FATF Standards requires countries to maintain an up to date assessment of their TF risks.** An important part of updating any assessment of TF risk will be to critically review the approach taken, and to identify areas for improving the approach the next time (e.g. identifying blind spots, areas where further information is needed), recognising that some jurisdictions may need to take a phased approach. Risk updates may focus on specific threats or sectors, and/or the development of risk indicators.

78. **While a risk assessment presents a snapshot in time, an assessment of TF risk should be an ongoing and evolving process.** Key competent authorities should be updating their analysis on an ongoing basis, taking into account current terrorism and TF threats and developments. Importantly, even jurisdictions that assess their domestic TF risk to be low should regularly update their assessment, and remain vigilant to changes in their terrorism and TF threat profile. **Jurisdiction experience highlights the particular benefits of embedding a culture of ongoing risk or threat assessment, having ongoing mechanisms to collect relevant information on TF risk, and conducting more targeted TF risk assessments which allow for enhanced stakeholder engagement** (e.g. focusing on specific sectors or threats, the development of risk indicators etc.). The textboxes below describe the approaches taken by the U.K. and Australia in updating their assessments of TF risk.

Box 5.1. The U.K.s updated 2018 ML/TF Risk Assessment[60]

In 2018 the U.K. completed an update to their 2015 ML/TF NRA. The first stage of the 2018 ML/TF risk assessment focused on identifying evidence which had emerged since the last NRA was conducted in 2015. Authorities found that the data gathering process for the NRA comprised mainly of extracting data from existing information or assessments from past and on-going work, rather than conducting new data gathering exercises. Through this process authorities identified the importance of embedding a culture of ongoing risk assessment: both UK NRAs benefitted from the wide range of ongoing risk and threat assessments used to inform operations, policy and resourcing. This meant that the NRAs could tie these together and analyse the findings in a cross-cutting way.

Box 5.2. Australia's Ongoing Approach to Assessing TF Risks

Since Australia's last NRA in 2014, the country has moved away from the broad-scope, "all-in", model towards a sectoral-based or product-based assessment of TF and ML risk. Since 2016, AUSTRAC has completed[61]:

- five sectoral-based risk assessments (superannuation, financial planning securities and derivatives, NPOs and on-course bookmaker sectors)
- two product-based risk assessments (stored value cards and travellers cheques) and
- one issue-specific risk assessment (remittance corridors between Australia and pacific island countries).

Further assessments to be produced shortly include: Customer-owned banking (credit unions and building societies) as well as the broader banking sector. While this model requires countries to invest more time and investment than a one-off risk assessment, AUSTRAC has found that it enables a deeper and more focused analysis on each sector, product or issue. It also allows for a deeper engagement with industry sectors which helps to tailor the assessment and ensure it is a useful product in the longer term. This new approach has results in other additional benefits, such as: increased TF awareness and engagement by the sectors (including enhanced SMR reporting), identification of blind spots by industry and an awareness of where entities sit in the sector, and the provision of unique intelligence for partner agencies to inform national criminal threat reports.

60 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/655198/National_risk_assessment_of_money_laundering_and_terrorist_financing_2017_pdf_web.pdf

61 These reports are all available on AUSTRAC's website.

CONCLUSIONS

79. **While this Guidance highlights good approaches taken by jurisdictions in assessing TF risk, jurisdiction experience is continuing to evolve.** Likewise, the changing nature of TF threats and vulnerabilities means that relevant information sources which countries will need to consult when assessing TF risk will change to some extent over time. This report recognises that lower capacity jurisdictions often face additional challenges in assessing TF risk, despite terrorist organisations often targeting isolated communities within such jurisdictions for support. For such jurisdictions, it is vital that efforts to assess TF risk include community engagement, and consider broader criminal networks and activities, which terrorist organisations often draw on to raise, and move, funds or other assets. This report has highlighted a number of examples of regional information sharing initiatives on TF. Such initiatives are vital to deepening the understanding of TF risk in certain regions, and going forward there is a need for enhanced information sharing on TF risk within regions which face similar TF threat profiles**.** This report also highlights that understanding TF risks linked to larger terrorism organisations as well as individual perpetrators often requires a close analysis of a large amount of financial data. For developed countries with large financial and trade flows, the development of smart solutions in order to cope with "big data" and the continued development of multi-agency information sharing mechanisms will likely be important in ongoing efforts to identify and assess TF risk.

Annex A. PUBLISHED TF RISK ASSESSMENTS AND OTHER RELEVANT OPEN SOURCES

Table A.1. Published National and Regional TF Risk Assessments

	National			
Jurisdiction	Year	TF standalone?	Link	Language
Armenia	2014 2017	no	ML/TF National Risk Assessment (Executive Summary) Analytical update of the 2014 Report on ML/TF National Risk Assessment	English
Australia	2014 2017 2017	Yes Yes no	Terrorism Financing in Australia National Risk Assessment of NPOs Remittance corridors: Australia to Pacific Island countries: money laundering and terrorism financing risk assessment *[A range of sector specific ML/TF risk assessments are also available on the AUSTRAC website.]*	English English English
Austria	2015	no	ML/TF National Risk Assessment - 2015	German
Bahamas	2016	no	National ML/TF Risk Assessment (Summary)	English
Belarus	2018	no	ML/TF National Risk Assessment (Summary)	Russian
Bhutan	2017	no	National ML/TF Risk Assessment	English
British Virgin Islands	2017	no	National Risk Assessment on ML/TF	English
Cambodia	2018	no	ML/TF National Risk Assessment (Sanitized)	English
Canada	2015	no	Assessment of Inherent Risks of ML and TF	English
Cayman Islands	2015	no	National Risk Assessment relating to ML, TF and PF	English
Chile	2016	No	National ML/TF Risk Assessment	Spanish
Colombia	2016	No	National ML/TF Risk Assessment – executive summary	Spanish
Cook Islands	2015	no	National Risk Assessment ML/TF	English
Czech Republic	2017	no	First round of National ML/TF Risk Assessment	English
Fiji	2015	no	ML/TF National Risk Assessment	English
Finland	2015	no	National Risk Assessment of ML/TF	Finnish
France	2017/2018	no	Trends and Analysis of ML/TF risks	French
Ghana	2016	no	National Risk Assessment on ML/TF	English
Greece	2019	no	National Risk Assessment Report on ML/TF	Greek
Hong Kong, China	2018	no	ML/TF Risk Assessment Report	English
Indonesia	2015	yes	National Risk Assessment ML/TF	Indonesian
Ireland	2016	no	National Risk Assessment ML/TF	English
Isle of Man	2015	no	National Risk Assessment of ML/TF	English
Israel	2017	yes	National Risk Assessment on TF (non-classified version)	English
Italy	2014	no	National Risk Assessment on ML/TF	English

	National			
Japan	2014	no	National Risk Assessment of ML/TF	English
Kyrgyzstan	2017	no	National Risk Assessment of ML/TF (summary)	Russian
Latvia	2018	no	Supplemented National ML/TF Risk Assessment Report	English
Lithuania	2015	no	National Risk Assessment of ML/TF	English
Luxemburg	2018	no	National Risk Assessment of ML/TF	English
Malta	2018	no	Results of ML/TF National Risk Assessment	English
Mexico	2016	no	National Assessment of ML/TF Risks	Spanish
Mongolia	2016	no	National Risk Assessment of ML/TF	English
Netherlands	2017 ongoing	Yes yes	National Risk Assessment on TF (summary) Netherlands Terrorism Threat Assessments	English English
New Zealand	2017	no	AML/CFT Sector Risk Assessment	English
Norway	2016	no	National Risk Assessment on ML/TF	Norwegian
Peru	2016	no	National Risk Assessment of ML/TF	Spanish
Philippines	2014 2017 2018	No No yes	First ML/TF National Risk Assessment Second National Risk Assessment on ML/TF National TF Risk Assessment of NPOs	English English
Portugal	2015	no	National Assessment of ML/TF risks	English
Russian Federation	2018	yes	National TF Risk Assessment	English
Seychelles	2017	no	National Risk Assessment Report for ML/TF	English
Singapore	2013 2019	No yes	National ML/TF Risk Assessment Report 2019 Terrorism Threat Assessment Report	English English
Slovak Republic	2017	no	Final Report on the National Assessment of the Risk of Money Laundering and Terrorist Financing in the Conditions of the Slovak Republic	English
Slovenia	2016	no	ML/TF Risk Assessment Report	English
Sri Lanka	2014	no	National ML/TF Risk Assessment (sanitized report)	English
Sweden	2014 2015 2017 2019	Yes Yes Yes Yes	National TF Risk Assessment Red Flag Report on Terrorist Financing Targeted TF Risk Assessment of Foreign Terrorist Fighters (FTFs) from Sweden and Denmark during 2013-2016 2019 Terrorism Threat Assessment	Swedish English English English
Switzerland	2015	no	Report on the National Evaluation of the Risks of ML/TF	English
Tajikistan	2017	no	National ML/TF Risk Assessment (summary)	Russian
Tunisia	2017	no	National Risk Assessment of ML/TF	English
Turks & Caicos Islands	2017	no	National ML/TF Risk Assessment	English
Uganda	2017	no	National ML/TF Risk Assessment	English
Ukraine	2016	no	National Risk Assessment report on preventing and countering legalization (laundering) of proceeds of crime and financing of terrorism	English

	National			
United Kingdom	2015 2017	yes	National Risk Assessment of ML/TF (2015) National Risk Assessment of ML/TF (2017)	English
United States	2015 2018	yes	National TF Risk Assessment (2015) National TF Risk Assessment (2018)	English
Vanuatu	2017	no	National Risk Assessment ML trough the Offshore Sector and TF	English
Zimbabwe	2015	no	ML/TF National Risk Assessment (summary)	English
	Regional			
Europe	2017 2019	yes	European Supranational Money Laundering & Terrorist Financing Risk Assessment -2017 European Union Terrorism Situation and Trend Report - 2019 (EUROPOL)	English
South East Asia and Australia	2016 2017	Yes Yes	Regional Risk Assessment on Terrorist Financing -2016 Non-profit organisations and terrorism financing: regional risk assessment 2018	English English

Table A.2. Other Relevant Open Source Resources

	Other Relevant Open Source Resources
General	Global Terrorism Database FATF Report on Emerging TF Risks (October 2015) FATF Report on Terrorist Financing in Central and West Africa (October 2016) FATF Report on Financing of Recruitment for Terrorist Purposes (January 2018) UNODC Guidance Manual for Member States on Terrorist Financing Risk Assessments OSCE Handbook on Data Collection in Supporting ML and TF National Risk Assessments
Foreign Terrorist Fighters	UNOCT Enhancing the Understanding of the Foreign Terrorist Fighters Phenomenon in Syria (July 2017)
Terrorist Organisations	FATF Report on Financing of ISIL (Feb 2015) FATF Report on Terrorist Financing in West Africa (2013)
Small cells and lone actors	Norwegian Defence Research Establishment (FFI) - The financing of jihadi terrorist cells in Europe (January 2015)

Note: The above list is not intended to be exhaustive, but provides examples of relevant open source resources.

Annex B. EXAMPLES OF RELEVANT COMPETENT AUTHORITIES AND TYPES OF USEFUL INFORMATION WHEN ASSESSING TF RISK

Assessing TF risk is a complex task for any jurisdiction, and it should utilize the broadest range of relevant information held by various domestic authorities. Key authorities that might have relevant information for preparing a TF risk assessment are categorized below; however, specific powers and types of information such authorities collect will likely vary between jurisdictions.

Type of authority	Information possessed by the authority, that might be useful for TF risk assessment
Law Enforcement Agencies	Information on domestic criminal context more generally. TF and terrorism-related investigations, interviews, testimonies, records of electronic communication and other intelligence or evidence that contains information about tools and methods used by terrorist or their facilitators to perform crimes. Information sent/received from foreign counterparts related to terrorism or TF. Criminal police records, international warrants, watch lists and other criminal databases. Domestic crime and terrorism related threat assessments.
Intelligence and Security Services	Intelligence and/or threat assessments related to domestic and international terrorist individuals and organisations, their *modus operandi* and facilitators. Intelligence on radicalised persons, high risk regions and areas outside and within jurisdiction, routes that are commonly used by FTFs, returnees or relocators to travel and other TF or terrorism related intelligence. Intelligence received from foreign counterparts.
Prosecution Authority	Convictions and verdicts in cases related to TF or terrorism, or other criminal cases linked to terrorists and their facilitators.
Financial Intelligence Unit	Suspicious Transaction Reports, Suspicious Activity Reports, including attempted transactions, threshold-based reports, bank account information, international wire transfers, beneficial ownership information, and other value-added operational analysis. Strategic analyses outcomes (TF typologies, sectoral risk assessments of reporting entities, supervised by FIU, etc.).
Immigration Authority	Aggregated data on immigrant inflows/outflows linked to high risk areas of terrorism or TF, Identity Documents, intended place of stay, intended place of work of the foreign terrorist,.
Customs Authorities	Cross-Border Cash/BNI Declarations or Disclosures, intelligence on cross-border cash and goods smuggling, information on types of cargo that are transported and links to terrorist individuals and organisations.
Border Security Authority	Travel data (flight/ships manifests, passenger name records). Hubs and entry points that are used by terrorists and their facilitators or might be vulnerable to them, intensity of trips, modes of transport used.

Type of authority	Information possessed by the authority, that might be useful for TF risk assessment
Ministry of Foreign Affairs	Information on UN sanctions lists and related requests sent/received, assessment of the international terrorism, TF and crime threats.
Supervisory Authorities	Information on FIs/DNFBPs compliance with domestic AML/CFT regime, results of on-site/off-site inspections, aggregated data on international financial flows. Qualitative information on CTF vulnerabilities posed to different sectors and products. Information on the scale of unregulated activity.
NPO Supervisory Authority (if applicable)	Information on the scope and materiality of the sector, those NPOs that fall within the FATF definition, results of engagement and outreach to the sector, information about persons or otherwise who might have control of high-risk NPOs.
Ministry of Justice	TF or terrorism related mutual legal assistance requests sent or received by the jurisdiction.
Ministries of mines, trade or environment	Qualitative information on extraction/collection/mining sites and their potential misuse by terrorists or their facilitators.
Probation/Prison Service	Information related to terrorist activity in prisons, data on possible terrorists or their facilitators radicalized in prisons.
Tax and Revenue Authority	Annual financial statements and statements of purpose from NPOs subject to tax exemptions, data on the income, assets and property that are owned by suspected terrorists or their facilitators.
Social Welfare Administration	Qualitative information on potential vulnerabilities of social services for misuse by terrorists and their facilitators, information on background checks conducted for different services.
Company Registers	Name, address and other identification details of legal entities that might be incorporated by terrorists or their facilitators or otherwise linked to them. Information on the country of origin of beneficial owner(s) (if available). Qualitative information on types of legal persons or arrangements vulnerable to criminal misuse more generally.
Registry of Bank Account Holders	Data on bank accounts that are or were held by terrorists and their facilitators.
Motor Vehicle Registers	Data on motor vehicles (cars, motorbikes, ships, etc.) that are or were owned by terrorists and their facilitators.
Real Estate Registers	Data on various types of real property owned or rented by terrorists and their facilitators or property that was owned or rented by them.

Annex C. TERRORIST FINANCING RISK EVENTS: PRACTICAL TOOL

1. Understanding TF risks involves a consideration of known or suspected TF threats and vulnerabilities in the jurisdiction, and an understanding of how the threats and vulnerabilities interact. One approach to articulate the interaction of TF threats and vulnerabilities is the use of risk events. These are hypothetical scenarios derived from identified TF threats, vulnerabilities and consequences.

2. This practical tool provides further guidance on the use of risk events. The identified risk events can be taken into account in the analysis stage of the TF risk assessment. This includes assessing the nature, sources, likelihood and consequences of the possible risk events. It should be noted that the list of TF threats and vulnerabilities included in this Annex are examples only and are not intended to be exhaustive.

Identification of threats and vulnerabilities

3. The first step in the process is to identify jurisdiction-specific TF threats and vulnerabilities. It is best conducted with an open mind to brainstorm potential threats and vulnerabilities to ensure that the widest range of possible risk events are identified initially. These can then be refined based on the primary methods and payment mechanisms used, the key sectors which have been exploited, and the primary reasons why those carrying out the TF activities have not been apprehended or deprived of their assets. Chapter 2 of this Guidance includes further information on the identification of TF threats and vulnerabilities.

Combining threats and vulnerabilities into risk events

4. The second step in the process is to combine the identified threats and vulnerabilities into risk events. Threats and vulnerabilities can be combined in a number of different ways as different threats may seek to exploit more than one vulnerability in the jurisdiction. Some examples of combining threats and vulnerabilities into risk events are included in the table below.

Threats	Vulnerabilities	Risk Events
The nature and extent of the activities of domestic terrorist group X in the jurisdiction	Presence of individuals, groups or organisations that support or promote violent extremism	*Terrorist group X raises funds via cash donations obtained within the jurisdiction*
The nature and extent of the activities of domestic terrorist group X in the jurisdiction	Affiliates of banks circumvent international prohibitions that screen transactions for terrorists and terrorist financiers	*Terrorist group X moves funds out of the jurisdiction using wire transfers*
The nature and extent of the activities of foreign terrorist group Y in a neighbouring jurisdiction	Inadequate resources allocated to regulation of NPOs, given the risk level identified	*Foreign terrorist group Y uses domestic NPOs as fronts for terrorist financing activities*
The nature and extent of the activities of foreign	Weaknesses in the requirements concerning the	*Law enforcement are unable to investigate some TF cases*

Threats	Vulnerabilities	Risk Events
terrorist group Y in a neighbouring jurisdiction	identification of beneficial owners that are non-residents	*due to poor information about beneficial ownership and control of companies used by terrorists and terrorist financiers*
The nature and extent of the activities of foreign terrorist group Z in the region	Informal money transfer businesses are inadequately supervised for AML/CFT purposes	*Terrorist group Z moves funds through the jurisdiction via informal money transfer businesses to obscure the money flows*
The nature and extent of the activities of foreign terrorist group Z in the region	No measures or inadequate measures to freeze without delay terrorist funds and assets	*Terrorist group Z uses jurisdiction as a conduit for terrorist financing as the risk of funds and assets being frozen is low*
"Lone wolves" raising funds from legal or apparently lawful activities	TF not criminalised or inadequately criminalised	*Prosecutors are unable to prosecute the terrorist financier without a connection to a terrorist act or terrorist group*
"Lone wolves" raising funds from legal or apparently lawful activities	Inadequate co-ordination and information-sharing among law enforcement and intelligence agencies who combat TF	*Terrorist financier succeeds in self-funding a terrorist attack without being detected by authorities*

Annex D. EXAMPLES OF POTENTIAL INFORMATION SOURCES TO SUPPORT THE ASSESSMENT OF TF RISK FACING NPOs

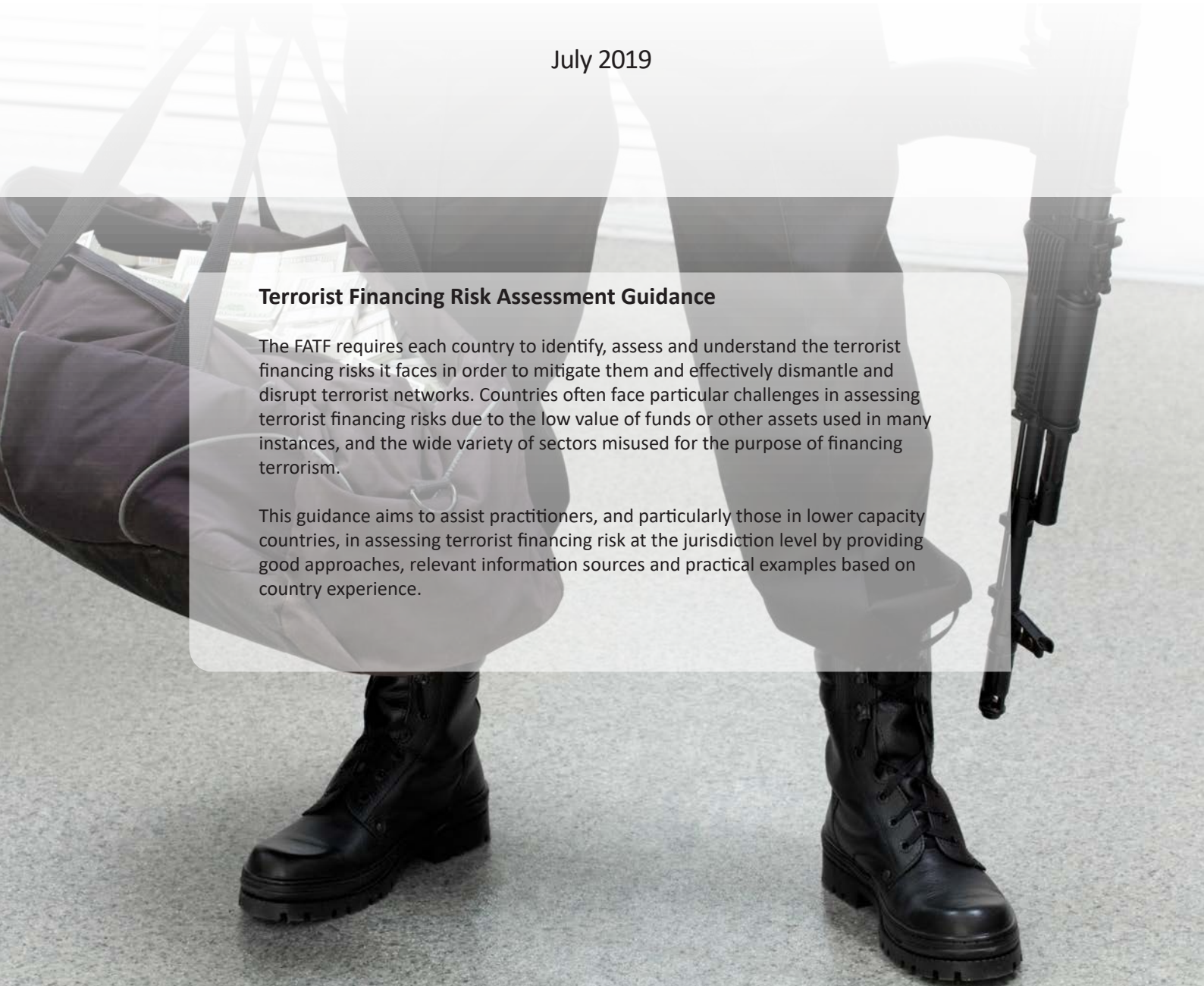
	Examples of Potential Quantitative Information	Examples of Potential Qualitative Information
Context Information on NPOs	• Data on the size and characteristics of the entire NPO sector, different categories of NPOs, and the subset of NPOs which fall within the definition. • Estimated Number of unregulated or informal NPOs. • Share (%) of GDP; value of funds raised and spent by the sector; • % of NPOs operating domestically and overseas; Incoming/ outgoing funds to NPOs (top 5 or 10 foreign donor jurisdictions) • Data on the inward and outward international financial flows linked to the NPO sector, e.g. through wire transfer reports • Data on the main NPO sources of funding and financial channels used to receive, store, move and use funds/donations. (e.g. bank transfers, MVTS etc.). • Data on tax filings from NPO sector, and public audit findings.	• Qualitative information on the types of legal forms of NPOs can adopt, characteristics, features, and activities of the NPOs (e.g. type and location of activities engaged in, and services provided). • Compatibility of national legislation concerning the formation of NPOs with FATF definition of NPOs (to identify those NPOs that fall within the FATF definition); • Qualitative information on the funding of NPOs (e.g. their donor base, types of funding, means of payment etc.).
Attractiveness for TF	• % of NPOs operating directly or indirectly in high risk jurisdictions for terrorism; • Value of funds sent to/received from high-risk jurisdictions for TF/terrorism.	• Online perceptions surveys or structured interviews with public sector experts and the NPO sector on potential TF vulnerabilities facing NPOs. • Review of terrorism or TF cases where NPOs are identified, and their role (organisational or sectoral vulnerabilities).
Terrorism and TF threat posed to those NPOs identified as vulnerable to TF	• Data on domestic terrorism and TF threat generally (e.g. number of active terrorist individuals and groups; number of TF investigations; volume of domestic population with communal ties to high-risk terrorism and conflict regions etc.) • Presence of domestic or regional terrorist individuals or entities with links to NPOs • the number of NPOs operating in proximity to a terrorist threat and/or high-risk populations • Incoming/outgoing foreign requests related to misuse of NPOs • Number of STRs, and terrorism/TF cases relating to NPOs	• Domestic and foreign Intelligence on terrorism threat and the potential misuse of NPOs • Online perceptions surveys or structured interviews with public sector experts and the NPO sector on the level of TF threat facing NPOs. • Domestic or international typologies on TF misuse and NPOs (and their applicability for the domestic context). • Open source information on links between NPOs and terrorist individuals or organisations (international reports).
Controls and prevention within organisations and within the sector	• Data on NPO supervision or monitoring if available (including self-regulatory mechanisms)	• strength of internal transparency and accountability practices concerning how funds are (i) collected; (ii) retained; (iii) transferred; (iv) spent; and (v) programs delivered as intended;

	Examples of Potential Quantitative Information	Examples of Potential Qualitative Information
		• Policy measures (including outreach and guidance to the sector on TF issues); • Qualitative information on the understanding of TF risks within the sector; • Due diligence and probity checks (donors, partners, and beneficiaries); • Online perceptions surveys or structured interviews with experts in authorities and the NPO sector.
National coordination and cooperation, and CTF capacity	• Volume and frequency of domestic exchange of information on NPOs.	• Qualitative information on coordination and cooperation between domestic authorities on information related to NPOs (designation of relevant contact points etc.). • Nature of domestic information requests. • NPO and TF expertise among competent authorities and within the sector; capacity to identify suspicious behaviour.

FATF

www.fatf-gafi.org

July 2019



Terrorist Financing Risk Assessment Guidance

The FATF 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. Countries often face particular challenges in assessing terrorist financing 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.

This guidance aims to assist practitioners, and particularly those in lower capacity countries, in assessing terrorist financing risk at the jurisdiction level by providing good approaches, relevant information sources and practical examples based on country experience.