FATF REPORT
Terrorist Financing Risk Assessment Guidance

July 2019

Purpose of the guidance

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.

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.

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.

FATF

Challenges to identify TF risk

1. Low value of funds and assets
2. Wide variety sectors misused
3. Cross-border nature of activity
4. Includes normal day to day activity e.g. Car hire, purchase of knife
5. Lack of expertise
6. Information gaps – due to unregulated unsupervised activities

2019 TFRA Guidance

- Builds on
  - FATFs 2013 Guidance on National Money Laundering and Terrorist Financing Risk Assessments
- Contains
  - Good approaches
  - Relevant information sources
  - Practical example for practitioners
- Draws on experiences and lessons learnt
  - Data from 35 jurisdictions
- One size does not fit all
  - Extract most relevant parts based on context and threat profile

Areas covered in the report

1. Key risk assessment considerations
2. Practical examples to overcome information sharing challenges
3. Provides examples of information sources for identifying threats and vulnerabilities
4. Provides Country contexts
   - Financial trade centres
   - Lower capacity jurisdictions
   - Bordering a conflict zone
5. Information sources for banks and MVTS
6. Good approaches for assessing NPO risk
7. Concludes on areas for further focus including
   - Enhanced information sharing
   - Continued development of information sharing initiatives
   - Tools for managing of big data

Country assessment

- Low risk assessment does not mean low risk
  - Low domestic terrorism risk but still face significant risk
- Need for ongoing risk assessment
  - Establish regular mechanisms to evaluate risk
  - Remain vigilant and monitor for changes to circumstances
- Identify blind spots
- Implementation of mechanisms to gather and collect qualitative and quantitative information

Objective of report

- Divided into five sections:

Part 1: Governance, Scoping and National Coordination - Good Approaches and Considerations

Part 2: Terrorist Financing Risk Methodologies - Good Approaches and Considerations

Part 3: Assessing Cross-border and Sector-specific Terrorist Financing Risks

Part 4: Non-Profit Organisations (NPOs) and Assessing Terrorist Financing Risk

Part 5: Follow up and Maintaining an Up-to-date Assessment of Terrorist Financing Risk

Key concepts and terms

- TF risk – a function of three factors
  - Threat
  - Vulnerability
  - Consequences

  Funds or assets (legitimate or illegitimate) raised, moved or stored in or through a jurisdiction
- TF threat
  - Persons with potential to cause harm raising, moving, storing or using funds and assets for terrorist activities (directly or indirectly involved)
- TF vulnerability
  - Things that can be exploited or support or facilitate terrorist activity - e.g. product or service, weaknesses in control measures
- TF consequences
  - Impact or harm that a TF threat may cause e.g. effect on the domestic and institutional financial system, the economy, society
  - Generally more severe than in the case of money laundering or financial crime
- TF risk assessment
  - Process or methodology to identify, analyse and understand the risk

Part 1: Governance, Scoping and National Coordination - Good Approaches and Considerations

Good approaches and considerations

Preliminary Scoping and Objective Setting

- 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.
- **In this regard, jurisdiction experience highlights the benefits of carrying out a scoping exercise prior to commencing an assessment of TF risk.**

Involvement of All Relevant Competent Authorities

- require involvement from a multitude of key authorities, across operational, policy and supervisory functions
- key authorities 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

Good approaches and considerations

Ongoing engagement with Non-Government Stakeholders

- Use of multi-stakeholder working groups and
- Public-private collaboration to assess terrorist financing risks
  - financial institutions,
  - designated non-financial businesses and professions (DNFBPs), and
  - non-profit organisations (NPOs)
- Engagement facilitated through open or closed online surveys, direct consultation, and existing umbrella organisations, facilitators or interlocutors to encourage dialogue

• Approaches Taken to Overcome Information-Sharing Challenges

- Effective inter-agency information sharing critical to ensure holistic and credible assessment of risks
- Ensuring jurisdictions have enabling policies and mechanisms permitting information sharing
- Establishing procedures and mechanisms to handle the exchange of sensitive information
- Ensuring that the lead agency is able to access and facilitate the sharing of sensitive information
- Exploring innovative ways to share information with competent authorities and non-government stakeholders

Part 2: Terrorist Financing Risk Methodologies - Good Approaches and Considerations

Good Approaches and Considerations

A risk methodology should be flexible, practical and take into consideration specific features and characteristics of the jurisdiction

Collecting a wide range of quantitative and qualitative information

- General criminal environment,
- TF and terrorism threats,
- TF vulnerabilities of specific sectors and products, and
- General CFT capacity

Domestic and foreign intelligence should be a key input

Take a holistic approach when considering terrorism threats

- TF risk may be linked to terrorism occurring in jurisdictions that are not within close proximity

Terrorist organisations and their facilitators have used similar methods as criminals to raise and move funds and other assets

Assess and continue to monitor TF risks regardless of the absence of known threats

Financial and non-financial supervisors as well as the non-government stakeholders important participants when assessing vulnerabilities

Part 3: Assessing Cross-border and Sector-specific Terrorist Financing Risks

Good practices

Consideration of both cross-border risks and TF risks posed to specific sectors

- Relevant information sources

Ongoing engagement with foreign counterparts

Sector-specific Terrorist Financing Risks

- Banking sector
- Money Value Transfer Services (MTVS)/Remittance sector
- Unregulated MVTS Providers and Hawala

Other Terrorist Financing Risks

- Exploitation of natural/environmental resources
- Extortion
- Variations in imports/exports
- Exposure of transit or end-user jurisdictions
- Movement of funds

The banking sector

- 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.
- The banking sector is subject to the most robust AML/CFT requirements (relative to other financial institutions).
- 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.

Terrorist Financing risk in the banking sector

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).

Terrorist Financing risk in the banking sector

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).

Part 4: Non-Profit Organisations (NPOs) and Assessing Terrorist Financing Risk

Examples of Considerations and Good Approaches

- Understanding the sector
- Identifying the nature and threat posed by terrorist organisations to NPOs deemed to be at risk
- Reviewing the adequacy of measures, including laws and regulations
- Engaging relevant competent authorities, the NPO sector and other non-government stakeholders
- Government agencies that have oversight over a part of the NPO sector (including regulators/supervisors, or self-regulatory bodies) need to play a central role
- Ongoing engagement with the NPO sector

Part 5: Follow up and Maintaining an Up-to-date Assessment of Terrorist Financing Risk

Good practices and considerations

- Findings of TF risk assessment endorsed by senior officials, and all key stakeholders have a common understanding of the outcomes
- Assessment of risk should result in clear and practical follow-up actions
- Maintain an up to date assessment
- An assessment of TF risk should be an ongoing and evolving process
- Embedding a culture of ongoing risk or threat assessment
- Ongoing mechanisms to collect relevant information on TF risk
- Conducting more targeted TF risk assessments which allow for enhanced stakeholder engagement

Conclusion

- TF risk, jurisdiction experience is continuing to evolve.
- The changing nature of TF threats and vulnerabilities means that relevant information sources will change over time.
- Lower capacity jurisdictions often face additional challenges in assessing TF risk.
- 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 highlights examples of regional information sharing initiatives that are vital to deepening the understanding of TF risk in certain regions,
- There is a need for enhanced information sharing on TF risk within regions which face similar threat profiles**.**
- This report also highlights that understanding TF risks often requires a close analysis of a large amount of financial data.
- Developed countries with large financial and trade flows, the development of smart solutions in order to cope with "big data" will likely be important in ongoing efforts to identify and assess TF risk.

Thank you

Roy Melnick
Financial Crime Risk Management Consultants

FCRMC
'effectively combatting financial crime'

Risk events practical tool

Terrorist financing risk events: Practical Tool

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 terrorist group Y in a neighbouring jurisdiction	Weaknesses in the requirements concerning the identification of beneficial owners that are non-residents	*Law enforcement are unable to investigate some TF cases due to poor information about beneficial ownership and control of companies used by terrorists and terrorist financiers*

Terrorist financing risk events: Practical Tool

Threats	Vulnerabilities	Risk events
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*

Competent authorities

Examples of relevant competent authorities and types of useful information when assessing TF risk

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.).

Examples of relevant competent authorities and types of useful information when assessing TF risk

Type of authority	Information possessed by the authority, that might be useful for TF risk assessment
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.

Examples of relevant competent authorities and types of useful information when assessing TF risk

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.

Examples of relevant competent authorities and types of useful information when assessing TF risk

Type of authority	Information possessed by the authority, that might be useful for TF risk assessment
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.