



COUNTERING THE FINANCING OF TERRORISM

Good Practices to Enhance Effectiveness

IN THIS MONTH'S ISSUE:

- ⇒ TERRORIST FINANCING (TF)
- ⇒ TERRORIST FINANCING RISK
- ⇒ GOOD PRACTICES TO ENHANCE EFFECTIVENESS
- ◆ THE ROLE OF THE PRIVATE SECTOR
- ◆ PRODUCING AND USING FINANCIAL INTELLIGENCE
- ◆ INVESTIGATING, PROSECUTING AND SANCTIONING OFFENDERS
- ◆ IMPLEMENTING TARGETED FINANCIAL SANCTIONS
- ◆ ENHANCED INTERNATIONAL COOPERATION
- ⇒ CASE STUDY

Terrorist Financing - What is it?

Terrorist financing is the earning, solicitation, collection, or provision of funds—from both legitimate (e.g. donations, business profits) and illegal sources (e.g. trafficking, fraud)—with the intent or knowledge that these funds will be used to support terrorist acts or organizations. Using funds and other assets involves not only the direct funding of terrorist attacks but also the funding of preparatory and support activities. Terrorist financing activities can include:

- The use of the financial services system to maintain and/or move funds which would be used to fund terrorist activities or organizations.
- The establishment of entities such as companies and non-profit organizations which can be used to collect, earn or raise funds for terrorism.

Legal Sources:

- * Business Profits;
- * Donations to charities or Non-profit organizations;
- * Community fundraising activities; and
- * Salaries.

Illegal Sources:

- * Drug trafficking;
- * Fraud and cybercrime;
- * Kidnapping for ransom;
- * Extortion; and
- * Smuggling (weapons, people and goods).

What is Terrorist Financing Risk?

Terrorist Financing (TF) risk is the potential for funds or assets to be solicited, collected, moved or used to support terrorist acts, organizations or individuals. Risk is typically assessed as functions of three (3) elements:

- * **Threats:** The potential for a person, entity or group to cause harm by raising, storing or using funds for terrorist purposes.
- * **Vulnerabilities:** Features in a jurisdiction or sector that can be exploited by terrorist groups, individuals or entities.
- * **Consequences:** The social, economic and political outcomes if a TF event occurs.

1. THREATS

- * Presence of terrorists;
- * Links to high-risk or sanctioned jurisdictions; and
- * History of terrorist activity.

2. VULNERABILITIES

- * Weak AML/CFT/CPF controls;
- * Poor customer due diligence processes; and
- * Limited oversight of non-profit organizations.

3. CONSEQUENCES

- * National security threats;
- * Loss of life;
- * Economic and reputational damages; and
- * International sanctions or blacklisting.

High-Risk Channels and Methods

Terrorists exploit various sectors to manage their financial activities such as:

- * **Non-Profit Organizations (NPOs):** This sector is often targeted due to its cash-intensive nature and the ease at which funds can be raised.
- * **Informal Financial Systems:** Systems such as **Hawala** provide anonymity and operate outside traditional banking regulations.
- * **Modern Technologies:** The increased use of Virtual Assets (Crypto), crowdfunding, gaming platforms and social media may be used for fundraising for terrorist activities.
- * **Traditional Assets:** Cash, gold or other precious metals may be used to move value across borders discreetly.

Key Good Practices

1. The role of Private Sector in mitigating TF risk.

- ◆ Adopt a Risk-Based Approach (RBA)
 - Conduct regular enterprise-wide terrorist financing (TF) risk assessments
 - Allocate stronger controls where risk is higher
 - Identify high-risk and sanctioned customers, products/services, geographic areas and delivery channels
- ◆ Strengthen Customer Due Diligence (CDD) Policies and Procedures
 - Encourage Financial Institutions (FIs) and Designated Non-Financial Businesses and Professions (DNFBPs) to implement and conduct proper Know Your Customer (KYC) procedures.
 - Regularly review and screen customer listing against Sanctions Lists such as those produced by the United Nations (UN) and the Office of Foreign Assets Control (OFAC).
 - Apply Enhanced Due Diligence (EDD) measures on Politically Exposed Persons (PEPs), NPOs and customers from High-risk jurisdictions such as North Korea and Iran.
 - Develop formal and informal information-sharing mechanisms with Regulators and Law Enforcement Agencies such as the White Collar Crime Unit (WCCU) and the Financial Intelligence Unit (FIU).
- ◆ Enhance knowledge of identifying suspicious transactions and reporting them through training with the Financial Services Regulatory Commission (FSRC) and the FIU.
- ◆ Develop partnerships with the Competent Authorities to improve communication and collaboration
- ◆ Governance and Oversight
 - Board and Senior Management must approve and implement CFT policies and procedures.



2. Mechanisms implemented by the Public Sector to mitigate TF Risk

- * The National Anti-Money Laundering Committee (NAMLC) has worked with the Attorney General's Office to develop and implement the Anti-Terrorism (Targeted Financial Sanctions Listing) Regulations, No. 13 of 2023 which make provisions for the designation, listing and delisting of persons, groups and entities associated with terrorist financing.
- * The Anti-Terrorism Act was amended in 2020 to insert Sections 114 – 119 which make provisions for Targeted Financial Sanctions (TFS) for the freezing without delay of funds or assets and reporting to the Attorney General's Office, the FIU and the FSRC.
- * The FSRC disseminates the UN and OFAC Sanctions Lists to all regulated entities when updated via email using office@fsrc.kn.
- * The FSRC in collaboration with the WCCU and the FIU have conducted training sessions on TFS for TF and conducting TF risk assessments.
- * In February 2025, the NAMLC, in collaboration with the Regional Security System—Asset Recovery Unit (RSS-ARU) organized a simulation exercise to test the national legislation, policies, procedures and mechanisms for TFS in relation to TF.
- * The NAMLC developed a National Standard Operating Procedure (SOP) for Targeted Financial Sanctions for Terrorist Financing and Proliferation Financing which provides Competent Authorities and relevant AML/CFT/CPF Agencies with step-by-step procedures on listing, delisting and freezing in relation to designated persons, entities and groups.



Core practices for enhancing effectiveness for Countering the Financing of Terrorism:

- ⇒ Public-Private Partnerships (PPPs): Establish formal frameworks for sharing information between regulated entities and law enforcement to better identify risks while enhancing detection.
- ⇒ Risk-Based Approach (RBA): Conduct comprehensive assessments to understand TF risks in sectors and tailoring and enhancing controls to align with the identified risks.
- ⇒ Financial Intelligence and Technology: Utilize technology to analyse transactions and improve the quality of Suspicious Transaction Reports (STRs).
- ⇒ International Cooperation: Implement robust mechanisms for coordination between regional and international bodies to detect, prevent, and prosecute MLTF/PF.
- ⇒ Focus on high-risk areas including the abuse of virtual assets and NPOs.

KINDLY REFER TO THE FSRC'S NEWSLETTER EDITIONS ON THE FOLLOWING RELATED TOPICS.

- ⇒ NOVEMBER 2025 - HAWALAS AND OTHER HOSSPS;
- ⇒ AUGUST 2025 - INFORMATION SHARING;
- ⇒ JULY 2025 - COMBATTING THE TERRORIST FINANCING ABUSE OF NGO/ NPOS; AND
- ⇒ APRIL 2023 - THE IMPORTANCE OF PUBLIC-PRIVATE PARTNERSHIP (PPP) IN AML/CFT/CPF.



Case Study – International NPO

The case demonstrates how Non-Profit Organizations (NPOs) can be abused to finance terrorism.

The Method: A domestic NPO held several accounts on which the NPO's founder had signing authority. Cash deposits and transfers were made into the accounts by donors, and the transfers always indicated that the funds were destined for a high risk jurisdiction. The domestic NPO then sent large wire transfers to a foreign-based international NPO.

Outcome: An investigation by the national law enforcement agencies revealed that the founder of the domestic NPO willfully used his role to facilitate the financing of terrorism and that the international NPO was the parent organization of the domestic NPO. The international NPO was suspected of being linked to a terrorist network and one of its contacts had been listed as a supporter of terrorism.

1. What are the vulnerabilities identified in the case?
2. What are some of the terrorist financing risks identified in the case?

Global Standards and Tools

- ◆ **FATF Recommendations:** The FATF sets International Standards that require countries to conduct National Risk Assessments (NRAs) to identify and mitigate their specific TF risks.
- ◆ **World Bank NRA Tool:** An analytical framework used by many countries to assess their inherent risks and the effectiveness of their controls.
- ◆ **Targeted Financial Sanctions (TFS):** Mechanisms used by the UN and national governments to immediately freeze the assets of designated terrorists.



REFERENCES

- ◆ IMF Library
- ◆ FATF-Gafi.org

South Independence Square Street, P. O. Box 898
Basseterre, St. Kitts, W.I.
Telephone No.: (869) 466-5048/
(869) 662-5940
Email: info@fsrc.kn
Website: www.fsrc.kn

