A HANDBOOK ON
ANTI-MONEY LAUNDERING AND
COUNTERING FINANCING OF TERRORISM
FOR NOT-FOR-PROFIT ORGANISATIONS
IN WEST AFRICA
A HANDBOOK ON ANTI-MONEY LAUNDERING AND COUNTERING FINANCING OF TERRORISM FOR NOT-FOR-PROFIT ORGANISATIONS IN WEST AFRICA

Produced by West Africa Civil Society Institute

Copyright © WACSI 2021
CONTENTS

ABOUT WACSI 5
ACKNOWLEDGEMENTS 5
ABBREVIATIONS AND ACRONYMS 7

1.0 INTRODUCTION TO THE CRIME OF MONEY-LAUNDERING, AND FINANCING OF TERRORISM 9
1.0 The Crime of Money Laundering, and Financing of Terrorism 10
1.1 Why criminals launder money 11
1.2 Why Non-profit actors need to understand Money Laundering and Financing of Terrorism regime 12
1.3 Origin of Money Laundering 12
1.4 Definitions of Key Concepts 13
1.5 Similarities & Differences Between Money Laundering & Terrorist Financing 20
1.6 Factors that Facilitate Money Laundering and Financing of Terrorism 21
1.7 Why AML/CFT? 26

2.0 THE ANTI-MONEY LAUNDERING AND COUNTERING FINANCING OF TERRORISM LEGAL FRAMEWORK 26
2.1 The global AML/CFT architecture 26

3.0 THE FINANCIAL ACTION TASK FORCE (FATF) 34
3.1 Objectives of the FATF 34
3.3 FATF Style Regional Bodies 37

4.0 THE FINANCIAL ACTION TASK FORCE (FATF) 40
4.1 Historical Background and Evolution of FATF Recommendations 41
4.2 Meaning and purpose of FATF Recommendations. 42
4.3 How does FATF ensure clear understanding of the 40 recommendations? 43
4.4 Recommendation 8 of the FATF 44
4.5 FATF Interpretive Note to Recommendation 8 for NPO knowledge, engagement, and advocacy 46
4.6 What is Recommendation 8 protecting? 47
## 5.0 DE-RISKING: WHAT NON-PROFIT ORGANISATIONS (NPOs) SHOULD KNOW

<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.1</td>
<td>What are the Key Drivers for De-Risking?</td>
</tr>
<tr>
<td>5.2</td>
<td>Effects of De-Risking on NPOs: Country Case Studies</td>
</tr>
</tbody>
</table>

## 6.0 THE INTER-GOVERNMENTAL ACTION GROUP AGAINST MONEY LAUNDERING IN WEST AFRICA (GIABA) AND NATIONAL FINANCIAL INTELLIGENCE UNITS (NFIU)

<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.2</td>
<td>The Role of GIABA in Implementation and Compliance of FATF Standards</td>
</tr>
<tr>
<td>6.3</td>
<td>National Intelligence Units in the GIABA Member States</td>
</tr>
</tbody>
</table>

## 7.0 THE FINANCIAL ACTION TASK FORCE (FATF) PROCESSES

<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.1</td>
<td>Mutual Evaluations</td>
</tr>
<tr>
<td>7.2</td>
<td>The National Risk Assessment</td>
</tr>
<tr>
<td>7.3</td>
<td>The National Sectoral Risk Assessment for NPOs</td>
</tr>
</tbody>
</table>

## 8.0 EFFECTIVE STRATEGIES TO PROTECT THE NPO SECTOR FROM VULNERABILITY TO TERRORIST FINANCING

<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.1</td>
<td>Building an Effective Self-Regulation Program</td>
</tr>
<tr>
<td>8.2</td>
<td>Building Effective AML/CFT Compliance Practices</td>
</tr>
</tbody>
</table>

## 9.0 HOW NON-PROFIT ORGANISATIONS (NPOs) CAN PARTICIPATE IN THE FATF PROCESS

<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.1</td>
<td>Conducting Non-Profit Organization Tailored Outreach</td>
</tr>
<tr>
<td>9.2</td>
<td>Perform NPO focused Mutual Monitoring.</td>
</tr>
<tr>
<td>9.3</td>
<td>Engaging in the National Risk Assessment Process</td>
</tr>
<tr>
<td>9.4</td>
<td>Engaging in the Mutual Evaluation Process</td>
</tr>
<tr>
<td>9.5</td>
<td>Gathering Evidence and Information</td>
</tr>
<tr>
<td>9.6</td>
<td>Raising NPO Awareness</td>
</tr>
<tr>
<td>9.8</td>
<td>Perform sector-led risk assessments for NPOs</td>
</tr>
</tbody>
</table>

## 10.0 BASIC UNDERSTANDING OF AML/CFT ISSUES FOR NON-PROFIT ORGANISATIONS

<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.1</td>
<td>Key NPO concerns with AML Regulations in Africa</td>
</tr>
<tr>
<td>10.2</td>
<td>What key actions can NPOs and Regulators take?</td>
</tr>
</tbody>
</table>
ABOUT WACSI

The West Africa Civil Society Institute (WACSI) was established by the Open Society Initiative for West Africa (OSIWA) in 2005 to reinforce the capacities of civil society in the sub-region. The institute became operational in July 2007. WACSI envisions a West Africa of efficient, effective, and influential civil society functioning as strategic partners for democracy, good governance, and sustainable national development. WACSI is a not-for-profit organisation that seeks to strengthen the institutional and operational capacities of civil society organisations through capacity strengthening programmes for increased and effective policy engagement, and the promotion of development, good governance, and democratic values in West Africa.

ACKNOWLEDGEMENTS

WACSI acknowledges the effort of leading contributors, Mr. Yona Wanjala, the Executive Director of Defenders Protection Initiative; Mr. Mulshid Eleas Muwonge Jr., the officer in charge of Special Projects and Strategic Initiatives at Defenders Protection Initiative; and Ms. Omolara Balogun, Head, Policy Influencing and Advocacy Unit at WACSI, for their thoroughness and commitment to putting this handbook together.

WACSI is also pleased to recognize staff members who coordinated the development of the Handbook including Omolara Balogun, John Frinjuah, and Ijeoma Kalu. The institute would like to thank the International Centre for Non-Profit-Law (ICNL) for their technical and financial support towards the development of this maiden edition of A handbook on Anti-Money Laundering and Countering of Financing of Terrorism for Non-Profit-Organisations In West Africa.

This Handbook was designed by: PIGMENT 0302545064
Copyright © WACSI 2021
## ABBREVIATIONS AND ACRONYMS

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AML</td>
<td>Anti-money laundering</td>
</tr>
<tr>
<td>CFT</td>
<td>Countering the Financing of Terrorism (also used for combating the financing of terrorism)</td>
</tr>
<tr>
<td>APG</td>
<td>Asia/Pacific Group on Money Laundering</td>
</tr>
<tr>
<td>CDD</td>
<td>Customer Due Diligence</td>
</tr>
<tr>
<td>CFATF</td>
<td>Caribbean Financial Action Task Force</td>
</tr>
<tr>
<td>CFT</td>
<td>Countering the financing of terrorism.</td>
</tr>
<tr>
<td>DNFBP</td>
<td>Designated Non-Financial Business or Profession</td>
</tr>
<tr>
<td>Egmont Group</td>
<td>The Egmont Group of Financial Intelligence Units</td>
</tr>
<tr>
<td>ESAAMLG</td>
<td>Eastern and Southern Africa Anti-Money Laundering Group</td>
</tr>
<tr>
<td>FATF</td>
<td>Financial Action Task Force on Money Laundering, Group d'action Financière sur le blanchiment de capital (GAFI)</td>
</tr>
<tr>
<td>FIU</td>
<td>Financial Intelligence Unit</td>
</tr>
<tr>
<td>FSRB</td>
<td>FATF Style Regional Bodies</td>
</tr>
<tr>
<td>GAFISUD</td>
<td>Financial Action Task Force on Money Laundering in South America</td>
</tr>
<tr>
<td>GIABA</td>
<td>Inter-Governmental Action Group against Money Laundering in West Africa</td>
</tr>
<tr>
<td>IAIS</td>
<td>International Association of Insurance Supervisors</td>
</tr>
<tr>
<td>IMF</td>
<td>International Monetary Fund</td>
</tr>
<tr>
<td>IN</td>
<td>Interpretive Note</td>
</tr>
<tr>
<td>IO</td>
<td>Immediate Outcome</td>
</tr>
<tr>
<td>KYB</td>
<td>Know Your Beneficiary</td>
</tr>
<tr>
<td>KYC</td>
<td>Know Your Customer</td>
</tr>
<tr>
<td>KYD</td>
<td>Know Your Donor</td>
</tr>
<tr>
<td>KYE</td>
<td>Know Your Employee</td>
</tr>
<tr>
<td>ML</td>
<td>Money Laundering</td>
</tr>
<tr>
<td>MONEYVAL</td>
<td>Council of Europe the Select Committee of Experts on the Evaluation of Anti-Money Laundering Measures</td>
</tr>
<tr>
<td>Acronym</td>
<td>Full Form</td>
</tr>
<tr>
<td>-------------</td>
<td>---------------------------------------------------------------------------</td>
</tr>
<tr>
<td>MOU</td>
<td>Memorandum of Understanding</td>
</tr>
<tr>
<td>NGO</td>
<td>Non-Government Organisation</td>
</tr>
<tr>
<td>NPO</td>
<td>Non-Profit Organisation</td>
</tr>
<tr>
<td>OAS</td>
<td>Organization of American States</td>
</tr>
<tr>
<td>PEP</td>
<td>Politically Exposed Person</td>
</tr>
<tr>
<td>R.</td>
<td>Recommendation</td>
</tr>
<tr>
<td>RBA</td>
<td>Risk-Based Approach</td>
</tr>
<tr>
<td>Special Rs</td>
<td>Nine Special Recommendations on Terrorist Financing issued by FATF</td>
</tr>
<tr>
<td>STR</td>
<td>Suspicious Transaction Report</td>
</tr>
<tr>
<td>TF Convention</td>
<td>The International Convention for the Suppression of the Financing of Terrorism 1999</td>
</tr>
<tr>
<td>TF</td>
<td>Terrorist Financing</td>
</tr>
<tr>
<td>The 40 Recommendations</td>
<td>The Forty Recommendations on Money issued by FATF</td>
</tr>
<tr>
<td>UN</td>
<td>United Nations</td>
</tr>
<tr>
<td>UNCAC</td>
<td>United Nations Convention against Corruption</td>
</tr>
<tr>
<td>UNODC</td>
<td>United Nations Office on Drugs and Crime</td>
</tr>
<tr>
<td>UNSC</td>
<td>United Nations Security Council</td>
</tr>
<tr>
<td>UNSCR</td>
<td>United Nations Security Council Resolutions</td>
</tr>
<tr>
<td>UNTOC</td>
<td>United Nations Convention against Transnational and Organised Crime</td>
</tr>
<tr>
<td>Vienna Convention</td>
<td>The United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances 1988</td>
</tr>
<tr>
<td>Wolfsberg Group</td>
<td>Wolfsberg Group of Banks</td>
</tr>
</tbody>
</table>
The Financial Action Task force (FATF) defines a non-profit organisation as *a legal person or arrangement or organisation that primarily engages in raising or disbursing funds for charitable, religious, cultural, educational, social, or fraternal purposes for the carrying out of other types of “good works.”*

Non-Profit Organisations (NPOs) perform a vital role in different communities worldwide, often remote, and challenging/hard to reach. Their functions may include but not limited to providing relief and support to groups of the population in need in urgent crisis; advocating for peace, democracy, and the rule of law in countries that suffer deficits of the same; striving for the realisation of human rights and fundamental freedoms and promoting a human rights culture in a non-violent way. Unfortunately, the FATF policy regulation has linked some non-profit organisation operations and funding to illicit sources and the facilitation of discrete processes and intent to finance terrorism.

**Recommendation 8** of the little-known FATF requires that the laws and regulations that govern non-profit organizations should be reviewed so that these organizations cannot be abused to finance terrorism.

While the Financial Action Task Force (FATF) - “Recommendation 8” was intended to protect the non-profit sector (NPOs/NGOs) from abuse, several countries around the world have and continue to use the FATF regulation as a seal of approval to justify undue restrictions towards the sector. Such has taken a draconian policy and administrative course ranging from increased state surveillance to foreign funding restrictions for peace, development, human rights, and fundamental freedoms advocacy work in some jurisdictions.

This handbook, therefore, seeks to facilitate learning among members of the non-profit sector about the critical money laundering and financing of terrorism key concepts, FATF 40 recommendations, with emphasis on Recommendation 8. The handbook also provides a broader understanding of the impact of FATF recommendations on global and national policies, focusing on government ML/FT regime, financial institutions De-risking policy measures, and the non-profit sector concerns. The book further presents some best practices in developing and implementing practical protocols to mitigate the sectors’ susceptibility to the risk of ML/FT.

The handbook affirms the need to equip the non-profit organisation with knowledge and skill in understanding ML/FT policy regulations, recognising the impact, and partnering
Global peace, security, and development are today more confronted by economic crimes of Money Laundering (ML), Financing of Terrorism (TF), and Proliferation Financing (PF) than ever before. These crimes do undermine jurisdictions, political and economic interests, and pose grave threats to national security. Thus, to fight these crimes effectively requires an all-inclusive approach where different stakeholders are presented with the opportunity to learn and participate, contribute to the knowledge and skills pool purposed at collective prevention, detection, and policing these crimes. Therefore, the non-profit actors ought to be taken as critical players in combating these financial crimes’ prevalence and not branded as perpetrators.

1.1 Why criminals launder money
It is a common practice that most person(s) who commit crimes of ML/TF try so much to prevent their actions before, during, and after the act, from being noticed by the law enforcement authorities and regulators. If the person(s) is arrested based on committing a crime of ML/FT, she/he will try to avoid having the criminal proceeds traced back to their illicit origin and prevent their confiscation. When such persons choose to spend the proceeds of their crime, they are engulfed in the dilemma of how to spend or invest large financial sums without evidence of a legitimate source of income, which could attract law enforcement authorities’ attention regulators. Alternatively, criminals’ ability to spend cash on the purchase and use of expensive goods or investments may still attract law enforcement authorities’ attention.

To spend illicit gains openly, criminals strive to ensure no apparent link between the profits of their crime and the actual illegal activities. Thus, all efforts aim to construct a believable cover story for an apparent legal origin of the illicit wealth. In this way, criminals seek to “launder” their illegal gains before spending or investing it in the economy.

According to the OECD training toolkit, terrorist organisations vary widely, ranging from large, state-like organisations to small, decentralised groups and self-directed networks. Terrorist attacks have also been committed by individuals who have found inspiration in radicalised environments or through self-radicalisation. These “lone actors” also need to fund their activities, and they may present challenges in identifying observable indicators. Therefore, raising and channeling the funds to facilitate acts of or terrorism is referred to as Terrorism Financing.
1.2 Why Non-profit actors need to understand Money Laundering and Financing of Terrorism regime

Recommendation 8 of the Financial Action Task Force (FATF, R.8) focuses on combating non-profit organisations’ abuse. Non-profit organisations play an essential role in the global economy. They complement the governmental and business sectors’ activities in providing services, comfort, and hope to the needy.

Unfortunately, the NPO sector has been exploited by terrorist organisations to provide financial and logistical support or otherwise support terrorist recruitments or terrorist operations. Recommendation 8 requires the regulators of NPOs to review the laws and legislations so that NPOs cannot be abused for financing terrorism.

This training toolkit, therefore, shall introduce you to the concept, definitions, origins, and development of Money Laundering, Financing Terrorism, Proliferation Financing, and other vital concepts. It further deals with factors that facilitate Money Laundering, Financing of Terrorism, and Proliferation Financing.

1.3 Origin of Money Laundering

Money Laundering dates to the 1920s when the organised criminals in the United States got much involved in profitable alcohol smuggling and began legalising their profits by blending it with the profits from a legitimate business.

According to Robinson, the term was first used in 1973 about the Watergate scandal. In that case, the dirty or illegal money was put through a series of transactions, and the money appeared clean or legal at the other end. The goal of money laundering is to serve the financial link between a crime and the persons behind that crime, allowing them to conceal the funds’ enjoyment.

1.4 Definitions of Key Concepts

1.4.1 What is Money Laundering?

It is imperative to note that there is no universally accepted definition of Money Laundering; however, there are various definitions of Money Laundering by the different authorities, some of which are indicated below;

Recommendation 8 of the Financial Action Task Force (FATF, R.8) focuses on combating the abuse of non-profit organizations. Non-profits play an important role in the global economy. They complement the activities of the governmental and business sectors in providing services, comfort and hope to the needy. Unfortunately, the non-profit sector has been exploited by terrorist organisations to provide financial and logistical support, or otherwise support terrorist recruitments or terrorist operations. Recommendation 8 requires the regulators of non-profit sector to review the laws and legislations to save the sector from abuse.
a. **The Financial Action Task Force (FATF)** defines Money Laundering as “the processing of criminal proceeds to disguise their illegal origin.”

b. **According to the International Monetary Fund (IMF),** Money Laundering is a “process in which assets generated or obtained by criminal activities are concealed or moved to create a link between the crime and the assets which are difficult to understand.”

c. **The United Nations, 2000 Convention Against Transnational Organized Crime**, also known as the Palermo Convention, defines money laundering as the conversion or transfer of property, *knowing it is derived* from a criminal offence, to conceal or disguise its illicit origin or of assisting any person who is involved in the commission of the crime to evade the legal consequences of his or her actions.

From the definitions above, it is clear that ML involves taking criminal proceeds and disguising their illegal sources to use the funds to perform legal or illegal activities. Simply put, money laundering is the process of making dirty money look clean by going through the **three stages** as below;

### 1.4.2 The Three Stages of Money Laundering

The Money Laundering process involves a complex and interconnected series of transactions. These are explained in the three typical stages of money laundering.

i. **Stage One: Placement**

This may involve the physical disposal of cash or other assets derived from criminal activity.

*Example of placement scenario*

K *(the money launderer)* introduces the illicit gains *(e.g. Cash from illegal narcotics sales, human trafficking, corruption, etc.)* into the financial system by placing the funds into circulation through formal financial institutions or other legitimate businesses, both domestic and international.

ii. **Stage Two: Layering**

This second stage of ML involves employing all launderer (s) tactics to separate the illicit gains from their source by layers of financial transactions intended to conceal the origin of the gains. This stage involves converting the proceeds of the crime into another form and creating complex layers of financial transactions to obfuscate the funds’ source and ownership.

*Example of a layering scenario*

K *(the money launderer)* electronically transfers money from country A to country B, from one financial institution to another by dividing the funds into advanced financial options. K may also choose to invest in real estate and other legitimate businesses or
place money in stocks, bonds, or life insurance products to create layers that separate the source’s illicit gains.

### iii. Stage 3: Integration
This involves positioning deceptive legitimacy to illicit gains or wealth through the re-entry of the funds into the economy in what appears to be regular business or personal transactions.

**Example of an integration scenario**
After layering the illicit gains, K (the money launderer) uses the illegal gains to invest in real estate, financial ventures, or luxury assets in what seemingly appears normal transactions to create a perception of legitimacy. By the integration stage, it is exceedingly difficult to distinguish between legal and illegal wealth.

**A visual representation of money laundering**

![Three Stages of Money Laundering](http://www.unodc.org/unodc/en/money-laundering/laundrycycle.html)

*Newcastle Business School*


### 1.4.3 Trends in Money Laundering
The traditional methods of money laundering have centred on the use of cash-based businesses, and this remains a crucial area. However, criminals will continue to seek out innovative methods to exploit weaknesses in the financial systems and to try to keep ahead of the investigators. Real estate, loans and trade-based money laundering are
known methods for criminals to launder the proceeds of crime. These will be described in detail at a later stage. More recent trends include:

a. **Cryptocurrencies** have, in a relatively short period, developed into a new payment method to store value. Financial transaction systems that are based on blockchain technology promise faster, cheaper, and anonymous transactions. The speed and global availability of cryptocurrencies, coupled with the limited regulations, the disaggregation of established financial intermediaries and the potential to hide the identity of the owners, make them an attractive method for criminals.

b. **Funnel accounts** refer to one or more bank accounts used for illegal funds deposited at one geographical location that gives criminals immediate access to the money via withdrawals in a different geographic location.

c. **Offshore bank accounts** of foreign legal entities continue to be used to make it difficult to track money flows. Overly complicated transactions or opaque ownership structures, including sequential or layered legal entities or trusts in multiple jurisdictions, including financial centres, persist. The purpose of these activities is to hide the origin of the funds and their beneficial owners.

d. **Professional enablers** and intermediaries (e.g. attorneys, accountants, trust and company services providers, notaries, estate agents, etc.) traditionally planned and created structures, based on their clients’ needs, whether for legitimate or criminal reasons. Their participation usually stops once the entities are formed and accounts opened. Over time, some professional enablers move beyond just establishing money laundering or tax evasion vehicles to actively managing their criminal clients’ illicit funds and providing money laundering as a service.

e. **Third-Party Money Laundering Groups** form part of an arrangement whereby a criminal organisation makes use of a third party for the laundering of its criminally derived proceeds. The Third-Party Money Laundering Group may establish intricate and durable means of “processing” its clients’ illicit funds, without exposure to or knowledge of the clients’ predicate offences. The criminal organisation pays a fee or commission. Otherwise, it does not have to deal with the efforts and risk associated with the money laundering activities, allowing it to focus on its criminal activities.

---

4 For a clinical examination of the money laundering process, the international extent of the problem and global efforts to introduce anti-money laundering measures and regulation in recent years, See: Buchanan, B. (2004). Money laundering—a global obstacle. Research in International Business and Finance, 18(1), 115-127.


1.4.4 What is Terrorist Financing?

Just like money laundering, there is no universal definition of Financing of Terrorism. However, some jurisdictions do have their guiding definitions as listed below.

a. Starting with the International Monetary Fund (IMF), Terrorism financing is defined as a process through which individual(s) or collect funds to apply those funds to the execution of terrorist deeds.\(^9\)

b. According to the World Bank, terrorism financing is defined as any form of financial support towards terrorism or those who conspire, participate and encourage the execution of terrorist deeds.\(^10\)

If simply defined, terrorism financing can be taken to mean financial support, in any form, of terrorism or of those who encourage, plan, or engage in terrorism. Unlike Money Laundering, which involves illicit funds, Financing of Terrorism uses both legitimate and illegitimate funds to facilitate an act of terror.

1.4.5 The terrorist financing process

The terrorist financing process is illustrated in the four steps as below:

---

**The Terrorist Financing Process**

- RAISING FUNDS
  - Donations
  - Self funding
  - Criminal activity

- TRANSFERING FUNDS
  - To a terrorist network
  - To a terrorist organization
  - To a terrorist cell

- USING FUNDS
  - Purchase weapons or bomb-making equipment
  - Payments for recruitment & training
  - Finance living expenses of terrorists

Funds used to finance terrorism are considered an ‘instrument of crime’ (which are either illicit or legitimate funds directed towards a criminal purpose).

*(AUSTRAC TF report 2014)*

Bank of Cyprus

---


This process involves:

a. Collecting the money for purposes of supporting the terrorist (from legitimate or illegitimate sources)

b. Storing the money while determining that its use is in line with the act.

c. Moving the money to the place and at the time it is needed.

d. Putting the money to use in advancing the terrorist organisation’s goals.

1.4.6 Trends in Terrorist Financing

A significant number of foreign fighters, having been both trained to fight and perhaps further radicalised in conflict zones, survived their combat engagements, exited the battlefield, and returned to their home country. The concern regarding returned foreign fighters is that they will commit acts of terror in their home or neighbouring countries. By referring suspicious behaviour and transactions to the appropriate authority, the tax administration can play a role in reducing the ability of terrorists and their financiers to commit these violent crimes.

Another trend involves the “lone actor” terrorist, which is very difficult to detect. Analysis in the aftermath of attacks has shown that weak signs and small financial traces can be observed. Tax examiners and tax auditors should be aware of this phenomenon and the specific circumstances surrounding it.

The radicalisation process can be challenging to detect and foresee. Radicalised individuals can be divided into two main groups. First, those known in connection with the extreme environment; and second, those inspired by radical ideas promoted by, for example, international terrorist organisations. Only very rarely can indications of this be observed unless there is direct contact with the person who is attempting to conceal their radicalisation.

The lone actor terrorist seeks to take control of the entire process him or herself. The goal of the process is usually to acquire the resources to commit an attack. Where small-scale attacks are chosen as the tactical option, the signs are generally not evident in the data that tax inspectors can analyse and audit. But where the attack has a more complex level, and the use of resources is somewhat higher, some indicators can be observed.

A lone actor terrorist may use complex efforts such as, tax and VAT fraud to build up capital to lend or provide real estate from where preparations can be made. The fraud will often use a registered company as a front. This company may also be used to acquire goods (e.g. fertilisers or other forms of chemicals or goods that should raise concerns or may even be subject to reporting by retailers). A company or several companies may be used further to cover the movement of goods to the attack site, and to cover or confuse investigators regarding the possible post-attack intentions, and to conceal the involvement of more personnel. By understanding the self-radicalised lone-actor
terrorist phenomenon, the tax administration can refer the case to the appropriate authorities.

1.5 Similarities & Differences Between Money Laundering & Terrorist Financing

According to ACAMS, Money laundering and terrorist financing are often mentioned in the same breath, without much consideration to the critically important differences between the two. The most fundamental difference between terrorist financing and money laundering involves the origin of the funds. Terrorist financing uses funds for an illegal political purpose, but the money is not necessarily derived from illicit proceeds. The purpose of laundering funds intended for terrorists is to support terrorist activities. The individuals responsible for raising funds are not the beneficiaries of the laundered funds. The money benefits terrorist activity.

On the other hand, money laundering always involves the proceeds of illegal activity. The purpose of laundering is to enable the money to be used legally. The individuals responsible for illegal activity are usually the ultimate beneficiaries of the laundered funds.

Graphical presentation of Similarities & differences between money laundering and terrorist financing

![Diagram showing similarities and differences between money laundering and terrorist financing]

Figure 3 - Adapted from OECD (2019), Money Laundering and Terrorist Financing Awareness Curriculum for Tax Examiners and Tax Auditors

1.6 Factors that Facilitate Money Laundering and Financing of Terrorism

The factors that facilitate Money Laundering and Financing of Terrorism may include
the following:14

i. **Lack of good governance**
The absence of accountable leadership, disregard for the rule of law/policies and the flourishing of corruption in any jurisdiction provides fertile grounds for the financial crimes of ML/TF.

ii. **Deficiency of Strong Monitoring Systems and Supervisory Mechanisms**
In most jurisdictions or institutions around the world, criminals or wrong dowers tend to exploit deficits entrenched in the financial systems to launder money or to facilitate activities related to the financing of terrorism. Such jurisdictions lack necessary capacity, systems and the like to implement compliance measures hence, extending to people an incentive to do wrong.

iii. **Lack of transparency**
Failure to institute a culture of accountability and transparency, duty bearers fail their responsibilities to members of staff. This has the potential to promote criminal practices like the laundering of money and financing of terrorism.

iv. **The widespread presence of illegal casinos**
Several typology research findings reveal several instances in which Casinos are open and shut down after a relatively short period. Such compounded by the fact that most managers and owners are foreigners, and several from high-risk jurisdictions can easily accelerate laundering through the investment of dirty funds in the establishment and operationalisation of the Casinos.

v. **The liberal nature of the real estate sector**
Most jurisdictions around the world, especially from developing countries, operate an unregistered and unregulated real estate business. Thus, measures like Know Your Customer (KYC), Customer Due Diligence (CDD) Know Your Beneficiary (KYB) and Know You Donor (KYD) procedures have no place by Real Estate agents.

vi. **Proximity to countries with illegal trafficking of gold and other precious stones.**
Publicly available information points to the illegal exploitation and smuggling of gold from Democratic Republic of Congo (DRC), Angola and the use of proceeds for laundering and funding other illicit activities, including the funding of terrorist organisations such as the Allied Democratic Forces (ADF) in Uganda.

vii. **Substantial legal privilege and confidentiality affecting authorities’ ability to extract information.**
Suspicious Transactions Reports (STR) and the financial institutions’ ability to perform effective customer due diligence (CDD) concerning beneficial owners of funds pooled in firms’ account is key to mitigating related ML/FT risks.

---

1.7 Why AML/CFT?

Money Laundering and Financing of Terrorism have severe economic, social and political consequences if they are not effectively combated. These crimes can significantly weaken national economies, financial systems, social fabric, collective ethical standards, and democratic institutions of society. The nature of these crimes is trans-national and known to thrive in jurisdictions with deficiencies in their Anti-Money Laundering (AML), Countering Financing of Terrorism (CFT) systems and framework. With the negative consequences of Money Laundering and Financing of Terrorism on national economies and financial systems, countries ought to dedicate all required efforts to fight them.\(^\text{15}\)

Money Laundering and the Financing of Terrorism can have devastating Economic and Social Consequences, which include but not limited to, the following:

a. **Reduction in Government Tax Revenue:** Money Laundering reduces tax revenue as it becomes problematic for the government to collect revenue from related transactions which frequently take place in the underground economy.

b. **Undermining the legitimate private sector:** Money launderers are known to use front companies in a bid to make their businesses appear legitimate and engage in a legitimate business. Still, they are controlled by criminals who commingle the proceeds of illicit activity with legitimate funds to conceal any the ill-gotten gains. These front companies have a competitive advantage over legitimate firms because they have access to substantial illicit funds, allowing them to subsidise products and services sold at below-market rates. This makes it difficult for legitimate businesses to compete against front companies.

c. **Weakening financial institutions:** Money Laundering and Financing of Terrorism can harm the soundness of a country’s financial sector. They can negatively affect the stability of individual banks or other financial institutions, such as securities firms and insurance companies.

Investors may not wish to invest in a country whose commercial and financial sectors are perceived to be compromised and subject to the influence of organised crime.

a. **Socio-cultural consequences:** Successful laundering of money creates the impression that crime pays, which encourages criminals to continue with their illicit schemes without any repercussions. This drives up the cost of government expenses and budgets due to the need for increased law enforcement and other expenditures to combat the severe consequences that result.

b. **Loss of life and destruction of property:** Successful Financing of Terrorism and

Proliferation Financing encourage acts of terrorism and war to prevail in society leading to significant loss of life and destruction of property.

c. **Reputation risk for the country:** A reputation as a Money Laundering and Financing of Terrorism can harm economic growth and development in a country. It diminishes legitimate global opportunities because foreign financial institutions find the extra scrutiny involved in working with institutions in Money Laundering havens too expensive.

d. **Risk of international sanctions:** To protect the financial system from Money Laundering, Financing of Terrorism and Proliferation Financing, the United Nations, the European Union, and other governing bodies may impose sanctions against foreign countries, entities or individuals, terrorists and terrorist groups, drug traffickers and other security threats.

Countries can be subject to comprehensive or targeted sanctions. Comprehensive sanctions prohibit all transactions with a specific country virtually. Targeted sanctions prohibit transactions with specified industries, entities, or individuals in the sanctioned country.

**Conclusion**

Money Laundering is the process where cash raised from criminal activities is made to look legitimate for re-integration into the financial system. In contrast, Financing of Terrorism cares little about the source of the funds, but it is what the funds are to be used for that defines its scope.

Money Laundering and Financing of Terrorism are both criminal offences with economic repercussions. They are global problems, their negative consequences undermine the stability, transparency, and efficiency of a financial system, provoke economic disturbances, jeopardise reform programs, result in diminished foreign investment and loss of a country’s reputation.

The most fundamental difference between Money Laundering and Financing of Terrorism involves the origin and purpose of the funds. Financing of Terrorism uses funds for an illegal political sense but may not be necessarily derived from illicit proceeds. On the other hand, Money Laundering and Proliferation Financing involve the proceeds of illicit activity.

Money Laundering and Financing of Terrorism have negative economic, social, and political consequences to society. These crimes affect the country’s economic growth and development, compromise the integrity of financial systems, and can even lead to loss of life. Therefore, countries must put in place robust mechanisms to combat these crimes to avert these negative consequences.
CHAPTER TWO

THE ANTI-MONEY LAUNDERING AND COUNTERING FINANCING OF TERRORISM LEGAL FRAMEWORK

2.1 The global AML/CFT architecture

The primary source of documents on Anti-Money Laundering (AML) and Countering the Financing of Terrorism (CFT) are the Legal instruments. They include among others, the United Nations Conventions and Security Council resolutions, the Financial Action Task Force (FATF) standards and best practices, the Egmont Group of Financial Intelligence Units (FIU) standards/best practices.16

All International efforts to curb Money Laundering and the Financing of Terrorism, are the reflection of a strategy purposed at attacking the economic power of the perpetrators of the transnational crimes, to weaken them by preventing usage of their illicit gains and averting the effects of the criminal economy and terrorism on the legal economy.

2.1.1 Examples of relevant international instruments and standards

There are three main categories of international instruments which include:

1. The United Nations Conventions and Resolutions
2. United Nations Counter-Terrorism Strategy
3. Financial Action Task Force Standards
4. The European Union Directives on Anti Money Laundering

European Union Directives on Money Laundering – European Union issues directives which are adopted by the Council, requiring member states to achieve (by amending national law, if necessary) the specified results. For instance, the “First Directive” required the members to enact legislation to prevent their domestic financial systems from being used for Money Laundering.

The European Union is unique by nature because it is a community of states. This makes it fundamentally different from other international organisations. The European Union can adopt measures that have the force of law even without the approval of the national parliaments of the various member states. European law prevails over national law in the case of directives. In this respect, European Union Directives have far more weight than the voluntary standards issued by groups such as the Basel Committee or Financial Action Task Force. Of course, the directive applies only to European Union member states and not to other countries.

---

16 The Egmont Group of Financial Intelligence Units is an international organization that facilitates cooperation and intelligence sharing between national financial intelligence units to investigate and prevent money laundering and terrorist financing. See also, https://egmontgroup.org/en
2.1.2 Select UN Normative Instruments for combating AML/CFT

Several instruments were enacted under the UN auspices as below.


This came into force in September (2003) to widen the scope of the Money Laundering offence. It was enacted thereunder that Money Laundering should not only apply to the proceeds of illicit drug trafficking but should also cover the proceeds of all serious crimes. It also urged member states to create a comprehensive domestic supervisory and regulatory regime for banks and non-financial institutions, including, natural and legal persons as well as any entities particularly susceptible to being involved in a Money Laundering scheme. The convention also calls for the establishment of Financial Intelligence Units (FIUs).\(^{17}\)

b. **The United Nations Convention against Corruption (Merida Convention)**

This came into force in December (2005) to widen the scope of Money Laundering. Under this convention, it was stipulated that Money Laundering should not only apply to the proceeds of illicit drug trafficking but should also cover the proceeds of all serious crimes. It also urged member states to create a comprehensive domestic supervisory and regulatory regime for banks and non-financial institutions including natural and legal persons as well as any entities particularly susceptible to being involved in a Money Laundering scheme.\(^{18}\) The convention also calls for the establishment of Financial Intelligence Units (FIUs).\(^{19}\)

c. **The International Convention for the Suppression of the Financing of Terrorism.**

This came into force in April (2002), with a requirement that all Member States take or put in place measures to protect their financial systems from being misused by persons planning or engaged in terrorist activities. This was following the US terror events of September 11, (2001). Member States and jurisdictions, as a result, underlined the links between terrorism, transnational organised crime, the international drug trade and Money Laundering, and called on countries that had not done so to become parties to the relevant international conventions.\(^{20}\)

This led to the adoption of Resolution 1373 by the United Nations Security Council in September (2001) imposing certain obligations on the Member States, such as the prevention and the suppression of the financing of terrorist acts, the criminalisation of terrorism-related activities and of the provision of assistance to carry out those

---

19 For examples of the mandate of Financial Intelligence Units, see https://egmontgroup.org/en/content/financial-intelligence-units-fius
acts. The denial of funding and haven to terrorists and the exchange of information to prevent the commission of terrorist acts were also part of the set obligations. The Council, under the same resolution, also established the Counter-Terrorism Committee (CTC) to monitor the implementation of the resolution.

d. The United Nations Global Counter-Terrorism Strategy

This was adopted by the United Nations General Assembly on 8th September 2006, to fulfil the commitment made by world leaders at the September 2005 Summit, and to build on the elements proposed by the Secretary-General in his report dated 2-05-2006 titled “Uniting against Terrorism: Recommendations for a Global Counter-Terrorism Strategy.”

The strategy took the form of a Resolution (A/RES/60/288) and a Plan of Action. It is a unique global instrument formed to enhance national, regional, and international efforts to counter-terrorism. It was the first time that all Member States agreed to a familiar strategic approach to fight terrorism, not only sending a clear message that terrorism is unacceptable in all its forms and manifestation but also resolving to take practical steps individually and collectively to prevent and combat it. Those practical steps include a wide range of measures ranging from strengthening state capacity to counter terrorist threats to better coordination of the United Nation’s counter-terrorism activities.

2.1.3 Other Institutional frameworks for combatting AML/CFT

a. International association for insurance supervisors (IAIS)

This was established in 1994 to represent insurance regulators and supervisors in more than 130 countries, constituting 97% of the world’s insurance premiums.21

b. Basel committee on banking supervision

This was enacted to mainly deal with the procedure of customer due diligence for banks, and the process of sharing financial records between jurisdictions in connection with the fight against Financing of Terrorism.

c. Wolfsberg Principles

The Wolfsberg Standards consist of the various sets of Anti-Money Laundering principles, as well as related Statements, issued by the group since its inception.22

d. Financial action task force (FATF) standards

The Financial Action Task Force is an inter-governmental body whose purpose is the

---

21 It is the international standard-setting body responsible for developing and assisting in the implementation of principles, standards and other supporting material for the supervision of the insurance sector. The IAIS mission is to promote effective and globally consistent supervision of the insurance industry in order to develop and maintain fair, safe and stable insurance markets for the benefit and protection of policyholders and to contribute to global financial stability. Available at https://www.iaisweb.org/home

22 The Wolfsberg Group is an association of thirteen global banks which aims to develop frameworks and guidance for the management of financial crime risks. Available at https://www.wolfsberg-principles.com/
development and promotion of national and international policies to Combat Money Laundering and Financing of Terrorism.

e. **Wolfsberg Standards – Anti-Money Laundering Principles and Statements**

Financing of Terrorism addresses practices used by terrorists to finance their activities (such as the misuse of wire transfers, alternative remittance systems and non-profit organisations) and calls for the implementation of specific asset freezing, seizing and confiscation mechanisms.

These reference materials reflect the primary source documents on Anti-Money Laundering (AML) and Combating the Financing of Terrorism (CFT). The materials range from international legal instruments, such as United Nations Conventions and Security Council resolutions, to standards and best practices developed by bodies such as the Financial Action Task Force and the Egmont Group of Financial Intelligence Units.

2.1.4 **Summarising the global AML/CFT normative and institutional framework**

Table 1 - Examples of the Global AML/CFT Normative and Institutional Instruments

<table>
<thead>
<tr>
<th>Group</th>
<th>What is It?</th>
<th>Important Documents</th>
</tr>
</thead>
</table>
| Financial Action Task Force on Money Laundering | • Intergovernmental body with 34-member countries and two international organisations  
• Sets money laundering and terrorist financing standards | • 40 Recommendations on Money Laundering and Terrorist Financing (Last updated February 2012) |
| Basel Committee on Banking Supervision | • Established by the central bank governors of the G-10  
• Promotes sound supervisory standards worldwide | • Customer Due Diligence for Banks Paper (2001)  

23 The Wolfsberg Group n27 above
| European Union | • A politico-economic union of 28-member states that are located primarily in Europe  
  • Issues AML/CFT directives regarding legislation that member states must issue to prevent their domestic financial systems being used for money laundering and terrorist financing | • First EU Directive on Prevention of the Use of the Financial System for Money Laundering (1991)  
  • Second Directive (2001)  
  • Third Directive (2005)  
  • Fourth Directive (2015) |
| Wolfsberg Group | • Association of 13 global banks Aims to develop standards on money laundering controls for banks | • Wolfsberg Anti-Money Laundering Principles for Private Banking (last updated 2002)  
  • The Suppression of the Financing of Terrorism Guidelines (2002)  
  • Anti-Money Laundering Principles for Correspondent Banking (2002) |
| APG, CFATF, EAG, GABAC, GIABA, GAFILAT, MENAFATF, MONEYVAL, ESAALMG | • FATF-style regional bodies that have similar form and functions to those of FATF.  
  • Provide input to FATF on standards and typologies. | • Typologies and so on |
| Egmont Group | • An informal networking group of financial intelligence units | • Statement of Purpose (last updated 2004)  
  • Principles for Information Exchange Between Financial Intelligence Units for Money Laundering Cases (2001)  
| CICAD | • Commission within the Organization of American States that deals with drug-related issues, including money laundering | • Model Regulations |
| World Bank and International Monetary Fund | • These organisations work together and in conjunction with FATF to encourage countries to have adequate anti-money laundering laws and to review anti-money laundering laws and procedures of FATF member countries. | • Reference Guide to Anti-Money Laundering and Combating the Financing of Terrorism: A Manual for Countries to Establish and Improve Their Institutional Framework 2002 (revised 2007). |
**Conclusion**

In summary, the international Anti-Money Laundering/Countering Financing of Terrorism legal framework is comprised of the following laws:

- The United Nations Convention against the Illicit Traffic in Narcotic Drugs and Psychotropic Substances (Vienna Convention), (1988)
- The United Nations Convention against Corruption (Merida Convention).
- The International Convention for the Suppression of the Financing of Terrorism.
- The United Nations Global Counter-Terrorism Strategy, etc.
THE FINANCIAL ACTION TASK FORCE (FATF)

Founded in 1989, the Financial Action Task Force (FATF) is an inter-governmental body whose purpose is the development and promotion of policies, to combat money laundering and terrorist financing and other related threats to the integrity of the international financial system. The FATF is the world’s foremost anti-money laundering (AML) and counter-terrorism financing (CFT) regulator. While it has 39 official members and jurisdictions, it depends on the support of nine FATF-style regional bodies (FSRBs) to ensure that its policies extend to all corners of the world. Originally referred to as the G-7 Financial Action Task Force, today FATF serves as the vanguard in promulgating AML guidance to governmental bodies around the globe. Also, the International Monetary Fund (IMF) and the World Bank offer essential perspectives to the field.

It should be noted that the FATF has significantly influenced and changed the way the banking and business sectors around the world conduct their affairs. It also impacted on national laws, policy frameworks and operation of governments.24

3.1 Objectives of the FATF

The stated objectives of FATF’s are to “set standards and promote effective implementation of legal, regulatory and operational measures for combating money laundering, terrorist financing and other related threats to the integrity of the international financial system. Starting with its members, the FATF monitors countries’ progress in implementing the FATF Recommendations; reviews money laundering and terrorist financing techniques and counter-measures; and promotes the adoption and implementation of the FATF Recommendations globally.”

To fulfil these objectives, the FATF focuses on several critical tasks, which include the following:

1. **Spreading the AML message worldwide:** The group promotes the establishment of a global AML and anti-terrorist financing network based on the expansion of its membership, the development of regional AML bodies in various parts of the world and cooperation with other international organisations.

2. **Monitoring the implementation of the FATF 40 Recommendations among its members.** For example, in the year 2004, FATF started its third round of mutual evaluations of all its members and concluded this process in 2011. In 2014, FATF began its fourth round of mutual evaluations, which saw the adoption of a new

---

24 The secretariat of the intergovernmental body is based at the Organization for Economic Cooperation and Development (OECD) in Paris. FATF can be located online at http://www.fatf-gafi.org.
approach for assessing technical compliance with the Recommendations and effectiveness of the AML/CFT system among its members.

3.2 The FATF Methodology
The FATF new methodology was released in 2013, is greatly enriched by the practical experience of FATF, FATF-style regional bodies (FSRBs), the International Monetary Fund (IMF) and the World Bank in performing assessments of compliance with earlier versions of the FATF Recommendations. Collectively, the technical compliance and effectiveness assessments provide an integrated analysis of the extent to which the country is compliant with the FATF Recommendations and how successful it is in maintaining a strong AML/CFT system. It focuses on the following.

3.2.1 Technical Compliance
For the technical compliance component, the assessment team examines the implementation of the specific requirements of the FATF Recommendations, including the framework of laws and enforceable means, and the existence, powers and procedures of competent authorities. Generally, it does not include the specific requirements of the standards that relate principally to effectiveness. These are assessed separately through the effectiveness component of the Methodology.25

Examples of Compliance Ratings
For each Recommendation, assessors are expected to conclude the extent to which a country complies (or not) with the standard with a focus on four possible levels of compliance. These include: compliant, largely compliant, partially compliant, and non-compliant. In exceptional circumstances, a Recommendation may also be rated as not applicable. When deciding on the level of shortcomings for any Recommendation, assessors are encouraged to consider the country context, the number and the relative importance of the criteria met or not met.

3.2.3 Effectiveness
Just like technical compliance, the assessment of the effectiveness of a country’s AML/CFT system is equally as important. The primary goal of an assessment of effectiveness is to provide an appreciation of the whole of the country’s AML/CFT system and how well it works. The approach of assessing effectiveness is fundamentally different from that of assessing technical compliance with the Recommendations. It does not entail checking whether specific requirements are met, or that all elements of a given Recommendation are in place. Instead, it requires a judgement as to whether, or to what extent defined outcomes are being achieved, i.e., whether the critical objectives of an AML/CFT system, in line with the FATF Standards, are being effectively met in practice the assessment process is reliant on the judgement of assessors, who will work
in consultation with the assessed country.26

3.2.4 The Framework for Assessing Effectiveness

To give the right balance between an overall understanding of the effectiveness of a country’s AML/CFT system, and a detailed appreciation of how well its parts are operating, the FATF assesses effectiveness primarily based on eleven Immediate Outcomes. Each of these represents one of the key goals which an effective AML/CFT system should achieve, and they feed into three Intermediate Outcomes which represent the primary thematic goals of AML/CFT measures. Assessors are not expected to evaluate the High-Level Objective or Intermediate Outcomes directly. However, these could be relevant when preparing the written MER and summarising the country’s overall effectiveness in general terms.

*It is essential to note that it is the responsibility of the assessed country to demonstrate that its AML/CFT system is effective. If the evidence is not made available, assessors can only conclude that the system is not effective. Assessors’ conclusions on the level of effectiveness should be primarily descriptive. For each Immediate Outcome, there are four possible ratings for effectiveness, based on the extent to which the core issues and characteristics are addressed: High level of effectiveness; Substantial level of effectiveness; Moderate level of effectiveness; and Low level of effectiveness.*27

3.3 FATF Style Regional Bodies

3.3.1 Principles guiding FATF-Style Regional Bodies

The FATF-style regional bodies (FSRBs) also considered FATF associate members are nine in number and have similar forms and functions to those of FATF. While FATF remains the only standard-setting body as per its objective, the setting of the standards greatly depends on information from the FSRBs as much as from its members. High-Level Principles and Objectives, which lays out the relationship between the FATF and FSRBs, was approved by the FATF Plenary in October 2012.

*Table 2 - High-Level Principles: Adapted from Sygna: What are the 9 FATF-Style Regional Bodies (FSRBs)*

<table>
<thead>
<tr>
<th>Principle</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Standard Setting</td>
<td>The FATF is the only entity allowed to set standards, but it relies on the help of FSRBs to do it well.</td>
</tr>
<tr>
<td>Technical Assistance</td>
<td>FSRBs can play a vital role in establishing and addressing the AML/CFT technical needs of their members, which supports the overall aims of the FATF.</td>
</tr>
</tbody>
</table>
### Autonomy

FATF and FSRBs are unique, free-standing, and autonomous parties, with no organisational hierarchy between them. Each party has different needs and experiences and therefore helps to strengthen global AML/CFT policy.

### Sharing common objectives and working in partnership

While the FATF and FSRBs operate independently of each other, they are also interdependent in the sense that they have a common goal (AML/CFT) which requires them to work together to maximise their results. The failure or success of either the FATF or FSRBs affects the other.

### Mutuality

The organisations’ reliance on each other ensures that the FATF and FSRBs establish operations and procedures that allow them to work together and take part in the other’s activities.

### A shared interest in protecting the FATF brand

As FATF-Style Regional Bodies (FSRBs) share such a close association with the FATF, they are obligated to uphold the values and name of the FATF to strengthen their brands.

#### 3.3.2 Geographical Jurisdiction of FATF Styled Regional Bodies

The 9 FATF-Style Regional Bodies help construct and support AML/CFT compliance policies and updates in every major region in the world. FSRBs disseminate the FATF’s global standards to help the 200+ countries under their jurisdictions understand and comply with FATF’s AML/CFT expectations.

*Figure 4 – Adapted from SYGNA - What are the 9 FATF-Style Regional Bodies (FSRBs)?*
CHAPTER FOUR

THE FINANCIAL ACTION TASK FORCE (FATF) 40 RECOMMENDATIONS

A key element of FATF’s efforts is its detailed list of appropriate standards for countries to implement. These measures are set out in the 40 Recommendations, which were first issued in 1990 and revised in 1996, 2003 and 2012. FATF has also issued various Interpretative Notes designed to clarify the application of specific Recommendations and to provide additional guidance.

After the events of September 11, 2001, FATF adopted and published the FATF IX Special Recommendations on terrorist financing. The first eight Special Recommendations were adopted on October 31, 2001, and the ninth on October 22, 2004. The 2012 revisions combined the IX Special Recommendations into the 40 Recommendations as clustered below.

Table 3 - An overview of the FATF 40 Recommendations

<table>
<thead>
<tr>
<th>Group</th>
<th>Topic</th>
<th>Recommendations</th>
</tr>
</thead>
</table>
| I     | AML/CFT Policies and Coordination  
  • Assessing risks and applying a risk-based approach  
  • National cooperation and coordination | 1–2 |
| II    | • Money Laundering and Confiscation  
  • Money laundering offences  
  • Confiscation and provisional measures | 3–4 |
| III   | • Terrorist Financing and Financing of Proliferation  
  • Terrorist financing offences  
  • Targeted financial sanctions related to terrorism and terrorist financing.  
  • Targeted financial sanctions related to proliferation Non-profit organisations | 5–8 |
| IV    | • Financial and Nonfinancial Institution Preventative Measures  
  • Financial institution secrecy laws  
  • Customer due diligence and record-keeping  
  • Additional measures for specific customers and activities  
  • Reliance, controls, and financial groups  
  • Reporting of suspicious transactions  
  • Designated non-financial businesses and professions | 9–23 |
### 4.1 Historical Background and Evolution of FATF Recommendations

In response to mounting concern over money laundering, the Financial Action Task Force on Money Laundering (FATF) was established by the G-7 Summit that was held in Paris in 1989. Recognising the threat posed to the banking system and to financial institutions, the G-7 Heads of State or Government and President of the European Commission convened the Task Force from the G-7 member States, the European Commission and eight other countries.

The Task Force was given the responsibility of examining money laundering techniques and trends, reviewing the action which had already been taken at a national or international level, and setting out the measures that still needed to be taken to combat money laundering. In April 1990, less than one year after its creation, the FATF issued a report containing a set of Forty Recommendations, which were intended to provide a comprehensive plan of action needed to fight against money laundering. In 2001, the development of standards in the fight against terrorist financing was added to the mission of the FATF. In October 2001, the FATF issued the Eight Special Recommendations to deal with the issue of terrorist financing. The continued evolution of money laundering techniques led the FATF to revise the FATF standards comprehensively in June 2003.

In October 2004, the FATF published a Ninth Special Recommendations, further strengthening the agreed international standards for combating money laundering and terrorist financing - the 40+9 Recommendations.

| V  | • Transparency and Beneficial Ownership of Legal Persons and Arrangements  
• Transparency and beneficial ownership of legal persons  
• Transparency and beneficial ownership of legal arrangements | 24–25 |
|---|---|
| VI | • Powers and Responsibilities of Competent Authorities and Other Institutional Measures  
• Regulation and supervision  
• Operational and law enforcement  
• General requirements  
• Sanctions | 26–35 |
| VII | • International Cooperation  
• International instruments  
• Mutual legal assistance  
• Mutual legal assistance regarding freezing and confiscation  
• Extradition  
• Other forms of international cooperation | 36–40 |
In February 2012, the FATF completed a thorough review of its standards and published the revised FATF Recommendations. This revision is intended to strengthen global safeguards and further protect the integrity of the financial system by providing governments with stronger tools to take action against financial crime. They have been expanded to deal with new threats such as the financing of proliferation of weapons of mass destruction, and to be clearer on transparency and tougher on corruption. The 9 Special Recommendations on terrorist financing have been fully integrated with the measures against money laundering. This has resulted in a stronger and clearer set of standards.

4.2 Meaning and purpose of FATF Recommendations.
The FATF Recommendations set out the essential measures that countries should have in place to:

<table>
<thead>
<tr>
<th>Ref</th>
<th>Purpose for 40 Recommendations</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.1</td>
<td>Identify the risks, and develop policies and domestic coordination;</td>
</tr>
<tr>
<td>1.2</td>
<td>Pursue money laundering, terrorist financing and the financing of proliferation</td>
</tr>
<tr>
<td>1.3</td>
<td>Establish powers and responsibilities for the competent authorities (e.g., investigative, law enforcement and supervisory authorities) and other institutional measures;</td>
</tr>
<tr>
<td>1.4</td>
<td>Apply preventive measures for the financial sector and other designated sectors;</td>
</tr>
<tr>
<td>1.5</td>
<td>Enhance the transparency and availability of beneficial ownership information of legal persons and arrangements;</td>
</tr>
<tr>
<td>1.6</td>
<td>Facilitate international cooperation.</td>
</tr>
</tbody>
</table>

4.3 How does FATF ensure clear understanding of the 40 recommendations?
a. The FATF Standards comprise the Recommendations themselves and their Interpretive Notes, together with the applicable definitions in the Glossary. The measures set out in the FATF Standards should be implemented by all members of the FATF and the FSRBs, and their implementation is assessed rigorously through Mutual Evaluation processes, and through the assessment processes of the International Monetary Fund and the World Bank - based on the FATF’s common assessment methodology. Some Interpretive Notes and definitions in the glossary include examples which illustrate how the requirements could be applied. These examples are not mandatory elements of the FATF Standards and are included for guidance only. The examples are not intended
to be comprehensive, and although they are helpful indicators, they may not be relevant in all circumstances.

b. The FATF also produces Guidance, Best Practice Papers, and other advice to assist countries with the implementation of the FATF standards. These other documents are not mandatory for assessing compliance with the Standards, but countries may find it valuable to have regard to them when considering how best to implement the FATF Standards. A list of current FATF Guidance and Best Practice Papers, which are available on the FATF website, is included as an annex to the Recommendations.

c. The FATF is committed to maintaining a close and constructive dialogue with the private sector, civil society and other interested parties, as important partners in ensuring the integrity of the financial system. The revision of the Recommendations has involved extensive consultation and has benefited from comments and suggestions from these stakeholders. Going forward and in accordance with its mandate, the FATF will continue to consider changes to the standards, as appropriate, in light of new information regarding emerging threats and vulnerabilities to the global financial system.

d. The FATF calls upon all countries to implement effective measures to bring their national systems for combating money laundering, terrorist financing and the financing of proliferation into compliance with the revised FATF Recommendations.

4.4 Recommendation 8 of the FATF

It must be recalled that in October 2001, the Financial Action Task Force drafted eight special recommendations on terrorist financing in response to a dynamic security threat that had culminated in the attacks made on September 11th of the same year. Originally referred to as Special Recommendation VIII (SR VIII), the current Recommendation 8, states that:

Countries should review the adequacy of laws and regulations that relate to entities that can be abused for the financing of terrorism. Non-profit organisations are particularly vulnerable, and countries should ensure that they cannot be misused:

a. by terrorist organisations posing as legitimate entities;

b. to exploit legitimate entities as conduits for terrorist financing, including to escape asset-freezing measures; and

c. to conceal or obscure the clandestine diversion of funds intended for legitimate purposes to terrorist organisations.

From the crafting of the R.8, it reveals that the FATF perceives non-profit organisations (NPOs) as vulnerable to numerous risks relating to both money laundering and terrorist financing like their for-profit counterparts, hence, SR VIII was designed to address specific terrorist financing vulnerabilities and threats faced by (NPOs).
When the revision of the FATF 40 Recommendations was performed in 2012, the final version integrated most of the Special Recommendations on terrorist financing into the general recommendations that address both anti-money laundering (AML) activities and activities meant to counter the financing of terrorism (CFT).

However, the FATF did recognise that out of the eight Recommendations, three of them remained unique to terrorist financing and grouped them in Section C of the Recommendations; former SR VIII, now Recommendation 8 (Measures to Prevent the Misuse of Non-profit Organisations), was one of the three.

Following the FATF typology study in 2000, several significant findings emerged from the analysis of 102 case studies submitted by FATF member states or compiled from open sources, as well as current research on the threat environment.\(^{28}\)

This forms the basis of FATF understanding for NPOs considering ML/FT, as stated below.

i. That the NPO sector has interconnected vulnerabilities, and terrorist entities seek to exploit more than one type of vulnerability. In the cases analysed for this project, the diversion of non-profit organisation funds by terrorist entities was a dominant method of abuse. However, other types of non-financial abuse, such as the abuse of programmes, or the support for recruitment, also appeared regularly.

ii. That the NPOs most at risk appear to be those engaged in ‘service’ activities, and that operate close to an active terrorist threat. This may refer to a non-profit organisation operating in an area of conflict where there is an active terrorist threat. However, this may also refer to a non-profit organisation that operates domestically, but within a population that is actively targeted by a terrorist movement for support and cover. In both cases, the critical variable of risk is not geographic, but the proximity to an active threat.

### 4.5 FATF Interpretive Note to Recommendation 8 for NPO knowledge, engagement, and advocacy

Non-profit organisations (NPOs) play a vital role in the world economy and in many national economies and social systems. Their efforts complement the activity of the governmental and business sectors in providing essential services, comfort and hope to those in need around the world. The ongoing international campaign against terrorist financing has unfortunately demonstrated, however, that terrorists and terrorist organisations exploit the NPO sector to raise and move funds, provide logistical support, encourage terrorist recruitment, or otherwise support terrorist organisations and operations. This misuse not only facilitates terrorist activity, but also undermines

---

donor confidence and jeopardises the very integrity of NPOs. Therefore, protecting the NPO sector from terrorist abuse is both a critical component of the global fight against terrorism and a necessary step to preserve the integrity of NPOs.

POs may be vulnerable to abuse by terrorists for a variety of reasons. NPOs enjoy the public trust, have access to considerable sources of funds, and are often cash intensive. Furthermore, some NPOs have a global presence that provides a framework for national and international operations and financial transactions, often within or near those areas that are most exposed to terrorist activity. Depending on the legal form of the NPO and the country, NPOs may often be subject to little or no governmental oversight (for example, registration, record keeping, reporting, and monitoring), or few formalities may be required for their creation (for example, there may be no skills or starting capital required, no background checks necessary for employees). Terrorist organisations have taken advantage of these characteristics of NPOs to infiltrate the sector and misuse NPO funds and operations to cover for, or support, terrorist activity.

4.6 What is Recommendation 8 protecting?
The objective of Recommendation 8 is to ensure that NPOs are not misused by terrorist organizations:

<table>
<thead>
<tr>
<th>Ref</th>
<th>Possible Area of Misuse</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.1</td>
<td>to pose as legitimate entities</td>
</tr>
<tr>
<td>1.2</td>
<td>to exploit legitimate entities as conduits for terrorist financing, including for the purpose of escaping asset freezing measures</td>
</tr>
<tr>
<td>1.3</td>
<td>to conceal or obscure the clandestine diversion of funds intended for legitimate purposes, but diverted for terrorist purposes</td>
</tr>
</tbody>
</table>

4.6.1 The 8 general principles guiding the implementation of recommendation 8

<table>
<thead>
<tr>
<th>Ref</th>
<th>Principle</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Past and ongoing abuse of the NPO sector by terrorists and terrorist organisations requires countries to adopt measures both: (i) to protect the sector against such abuse, and (ii) to identify and take effective action against those NPOs that either are exploited by, or actively support, terrorists or terrorist organisations.</td>
</tr>
<tr>
<td></td>
<td>Measures adopted by countries to protect the NPO sector from terrorist abuse should not disrupt or discourage legitimate charitable activities. Rather, such measures should promote transparency and engender greater confidence in the sector, across the donor community and with the public, that charitable funds and services reach intended legitimate beneficiaries. Systems that promote achieving a high degree of transparency, integrity and public confidence in the management and functioning of all NPOs are integral to ensuring the sector cannot be misused for terrorist financing.</td>
</tr>
<tr>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>3</td>
<td>Measures adopted by countries to identify and take effective action against NPOs that either are exploited by, or actively support, terrorists or terrorist organisations should aim to prevent and prosecute, as appropriate, terrorist financing and other forms of terrorist support. Where NPOs suspected of, or implicated in, terrorist financing or other forms of terrorist support are identified, the priority of countries must be to investigate and halt such terrorist financing or support. Actions taken for this purpose should, to the extent reasonably possible, avoid any negative impact on innocent and legitimate beneficiaries of charitable activity. However, this interest cannot excuse the need to undertake immediate and effective actions to advance the immediate interest of halting terrorist financing or other forms of terrorist support provided by NPOs.</td>
</tr>
<tr>
<td>4</td>
<td>Developing cooperative relationships among the public, private and NPO sector is critical to raising awareness and fostering capabilities to combat terrorist abuse within the sector. Countries should encourage the development of academic research on, and information-sharing in, the NPO sector to address terrorist financing related issues.</td>
</tr>
<tr>
<td>5</td>
<td>A targeted approach in dealing with the terrorist threat to the NPO sector is essential given the diversity within individual national sectors, the differing degrees to which parts of each sector may be vulnerable to misuse by terrorists, the need to ensure that legitimate charitable activity continues to flourish, and the limited resources and authorities available to combat terrorist financing in each country.</td>
</tr>
<tr>
<td></td>
<td>Flexibility in developing a national response to terrorist financing in the NPO sector is also essential, to allow it to evolve over time as it faces the changing nature of the terrorist financing threat.</td>
</tr>
</tbody>
</table>
5.1 What are the Key Drivers for De-Risking?

De-risking is defined as the practice of banks and other financial institutions exiting relationships with and closing the accounts of clients considered ‘high risk’. Non-profit organisations (NPOs), along with money-service businesses and correspondent banks, amongst others, are affected by de-risking. As a result, many NPOs around the world were or are unable to fulfil their mandate, impacting aid and relief, and lobbying for political and social change. It has also contributed to the transfer of funds through unregulated channels due to unnecessary delays or even the disappearance of funds transferred through controlled banking channels.

Furthermore, such stringent requirements have severely affected many NPOs, especially those who work in or around conflict zones. Grant payment transactions in support of local partners or disadvantaged communities arrive too late or do not meet them at all due to delays at banks and related banks, triggered by increased due diligence demands on the client, the customer’s partner or the beneficiaries.
<table>
<thead>
<tr>
<th>Driver</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Compliance with international rules and regulations for combating AML and CTF</td>
<td>The 40 FATF AML / CFT Recommendations, and in particular Recommendation 8 on the risk posed by NPOs for terrorist funding violence, have had various, often unintended, implications over the years and led to cases of over-regulation, including infringements of the fundamental democratic rights of association, assembly and speech. Several governments have issued tighter non-profit rules and restrictions based on the FATF standards, in many cases – further shrinking civic space.</td>
</tr>
<tr>
<td>National financial regulation</td>
<td>Financial regulators are tasked at the national level to ensure that regulation is in place to protect the integrity of the financial system. Central banks and other regulators in the financial sector must enforce monetary policies and provide Member Banks with regulatory and supervisory oversight. In the form of legislation, rules, and regulations, the strict global AML / CFT trickles down to the national level to improve the credibility of the financial sector in various jurisdictions.</td>
</tr>
<tr>
<td>Compliance requirements for banks</td>
<td>Financial institutions are required by law to disclose suspicious customers and transactions to competent authorities dealing with financial crime to comply with international laws and regulations to deter money laundering and terrorist funding through their payment systems. Banks have resorted to meticulous monitoring of their clients for the possibility of unwittingly encouraging money laundering or financing for terrorism. Consequently, Due Diligence (DD) regulatory activities and know your customer (KYC) to reduce financial and reputational risk has affected the partnerships between banks and non-profits worldwide. If banks determine (through a risk assessment) that the risk posed by a particular customer or sector is not worth the reward of banking those customers, they may decide to exit the relationship or not to enter into a relationship with them (De-Risk them). There is an emerging trend towards de-risking NGOs, forex offices, international embassies, and correspondent banks, as well as global politically exposed persons (PEPs), resulting in account closures in various countries. De-risking is partly an attempt on the part of banks to reduce their exposure to ML / TF risk, and possible litigation or fines/sanctions.</td>
</tr>
<tr>
<td>The United Nations Sanctions System</td>
<td>The United Nations Security Council has adopted several legally binding resolutions and has forbidden the financing of designated terrorist groups and their backers. Banks are expected not only to exclude from the financial system identified individuals and organisations but also their associates and networks. With more than 300 sanctions lists now in place worldwide, it is the risk management problem that emerges from possible interaction with designated parties that is key to de-risking and implicit decisions to cut financial services to persons. These stringent requirements ultimately trickle down to the ability of NPOs to access resources, especially for organisations working in conflict zones.</td>
</tr>
</tbody>
</table>
5.2 Effects of De-Risking on NPOs: Country Case Studies

![Map showing Brazil and Mexico](image)

**Figure 6 - Select Country Case Studies on Effects of De-risking**

<table>
<thead>
<tr>
<th>Country</th>
<th>De-risking Effects</th>
</tr>
</thead>
<tbody>
<tr>
<td>Brazil</td>
<td>In Brazil, the Petrobras scandal described as complicit in corruption, tax evasion and money laundering several large government-supported NGOs, or GONGO. The role of these GONGOs in the media has been widely publicised and has impacted the image of the entire NPO sector. Furthermore, support for human rights issues among the public is limited, as some of these issues are related to defending the rights of criminals. The corruption scandals have resulted in a more robust regulatory climate within Financial Institutions (FIs). Donations for NPOs come under these restrictions, with some FIs finding them more in need of investigation because of the corruption scandals in which they were involved (with public funds laundered by NPOs for private gain).</td>
</tr>
<tr>
<td>Mexico</td>
<td>Mexico's accountability of NGOs is a concern because of the corruption and tax evasion scandals associated with government related NPOs. Stakeholders find this question to be one of the reasons for banks and other financial institutions’ risk-averse attitude towards NPOs. A distinctive feature in Mexico is the involvement of drug cartels and organised crime, with considerable impact on the governance of the country, as well as on its economic and financial system through money laundering schemes that support a large part of the formal economy. NPOs receiving gifts from drug cartels for service delivery in deprived communities to build credibility within these populations are quite worried.</td>
</tr>
</tbody>
</table>
In Ireland, the legislative structure for charities in Ireland usually does not hinder NPO operations. However, there have been concerns about the Electoral Campaign Act, which was revised in 2001 to cover non-profit organisations' political activities, which tend to have an impact on the civil society operating space in Ireland. The amendment was inspired by anxieties regarding outside pressures on Irish politics. The legislation requires non-profits “committed to political activities” to register with the Electoral Commission; prohibits them from accepting funds from abroad; prohibits anonymous contributions over EUR 100 and forbids them from spending more than EUR 2500 on political campaigns or activities.
The Inter-Governmental Action Group against Money Laundering in West Africa (GIABA) was established on December 10, 1999, by a decision of the Authority of Heads of State and Government of the Economic Community of West African States (ECOWAS). The creation of GIABA is a significant response and contribution of the ECOWAS to the fight ML/FT. In January 2006, GIABA revised its mandate to fully incorporate and properly reflect its fight against the financing of terrorism.

Thus, GIABA is FATF-Styled Regional Body (FSRB) that is responsible for facilitating the adoption and implementation of Anti-Money Laundering (AML) and Counter-Financing of Terrorism (CFT) in West Africa. It works in collaboration with its member States to ensure compliance with international AML/CFT standards.

The objectives of GIABA are to:

- Protect the national economies and the financial and banking systems of signatory States against the proceeds of crime and combat the financing of terrorism;
- Improve measures and intensify efforts to combat the crime of ML/FT/PF;
- Strengthen cooperation amongst its members.

With sixteen-member states that subscribe to it, GIABA is also responsible for strengthening the capacity of member states towards the prevention and control of money laundering and terrorist financing within the ECOWAS. Apart from member states, GIABA grants Observer Status to African and non-African States, as well as Inter-Governmental Organisations that support its objectives and actions, and which have applied for observer status.
6.1 GIABA Member States

![Image showing GIABA Member States]

Figure 7- the GIABA Member States (Adapted from https://www.giaba.org/member-states/index_-1.html)

6.2 The Role of GIABA in Implementation and Compliance of FATF Standards

With the creation of GIABA Head of States and Governments of the ECOWAS established a specific mandate for the Inter-Governmental Organisation as follows:

a. To ensure the adoptions of standards against money laundering and the financing of terrorist, including the FATF 40 + 9 Recommendations.

b. To facilitate the adoption and implementation by member states of measures against ML and FT, taking into account specific regional peculiarities and conditions.

c. Function as a forum where members can discuss matters of regional interest and share experiences.

d. Organize self-evaluations and mutual evaluations to determine the efficacy of measures adopted, including their conformity to acceptable international standards.

e. Coordinate and provide support to member states to establish and implement AML/CFT regimes, including the implementation of laws against the proceeds of crime through mutual legal assistance, and in establishment and maintenance of financial intelligence units (FIUs).

The establishment of GIABA is a demonstration of good intention and desire of the ECOWAS Member States to the fight against money laundering and terrorist financing. In June 2006, GIABA was recognized as a Financial Action Task Force (FATF) Style
Regional Body (FSRB). In practice, GIABA operates on one hand as an ECOWAS specialized institution, and on the other hand as a Financial Action Task Force Style Regional Body. Apart from performing the core functions of a FSRB, including mutual evaluations to determine its members’ compliance with the FATF standards and typologies exercises to determine money laundering trends and methods, GIABA is the only FSRB with a technical assistance mandate.

6.3 National Intelligence Units in the GIABA Member States
Recommendation 29 of the FATF provides that, Countries should establish a financial intelligence unit (FIU) that serves as a national centre for the receipt and analysis of (a) suspicious transaction reports; and (b) other information relevant to money laundering, associated predicate offences and terrorist financing, and for the dissemination of the results of that analysis. The recommendation also provides that FIUs should be able to obtain additional information from reporting entities and should have access on a timely basis to the financial, administrative and law enforcement information that it requires to undertake its functions properly.

6.3.1 General Functions of FIUs
Though they vary in many ways, FIUs share a standard definition, which refers to their primary function: serving as a national centre for the collection, analysis, and dissemination of information regarding money laundering and the financing of terrorism. Below are the three shared core functions all FIUs recognised by the Egmont Group.

It should be noted that given their different status and history, it is not surprising that in some countries the FIU is entrusted with additional functions. For example, some FIUs monitor the compliance of specific entities with AML/CFT rules and standards. Other FIUs have the power to block reported suspicious transactions for a limited time. The FATF recommendations set a standard that countries should establish an FIU with the three core functions and contains other provisions that relate to the exercise of these functions. In contrast, no international norm or standard deals with the non-core functions of FIUs.

6.3.2 Examples of FIUs under GIABA’s Jurisdiction

Table 4 - Select FIUs under GIABA’s Jurisdiction

<table>
<thead>
<tr>
<th>Ref</th>
<th>Country</th>
<th>FIU</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Burkina Faso</td>
<td>The National Financial Information Processing Unit (CENTIF-BF)</td>
</tr>
<tr>
<td>2</td>
<td>Cape Verde</td>
<td>Cape Verde UIF (UIF)</td>
</tr>
<tr>
<td>3</td>
<td>Cote d’Ivoire</td>
<td>National Unit for the Processing of Financial Information in Côte d’Ivoire (CENTIF-CI)</td>
</tr>
<tr>
<td></td>
<td>The Gambia</td>
<td>Financial Intelligence Unit (FIU) of The Gambia</td>
</tr>
<tr>
<td>---</td>
<td>------------</td>
<td>-----------------------------------------------</td>
</tr>
<tr>
<td>5</td>
<td>Ghana</td>
<td>Financial Intelligence Centre Ghana (FIC)</td>
</tr>
<tr>
<td>6</td>
<td>Mali</td>
<td>National Financial Intelligence Processing Unit (CENTIF-Mali)</td>
</tr>
<tr>
<td>7</td>
<td>Niger</td>
<td>National Financial Intelligence and processing unit of Niger</td>
</tr>
<tr>
<td>8</td>
<td>Senegal</td>
<td>National Financial Intelligence Processing Unit (CENTIF)</td>
</tr>
<tr>
<td>9</td>
<td>Togo</td>
<td>Togo Financial Intelligence Unit (CENTIF Togo)</td>
</tr>
</tbody>
</table>

### 6.3.3 The Role of Financial Intelligence Centers or Units (FIC/FIU)

**Table 5 - General Functions of Financial Intelligence Units**

<table>
<thead>
<tr>
<th>Function</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Receiving Transaction Reports</td>
<td>The basic definition of the reporting obligation has two main aspects: which persons and entities are to be obligated to report and what is to be reported. Other aspects needing considerations include the form and contents of reports, rules relating to the reporting organisations, and means of enhancing the flow and quality of reports (including sanctions).</td>
</tr>
<tr>
<td>Analysing Reports</td>
<td>The second element of the core functions of an FIU, as defined by the Egmont Group, is the analysis of reports received from reporting entities.</td>
</tr>
<tr>
<td>Disseminating Reports</td>
<td>The third core function of an FIU is the dissemination of the information it has received and the sharing of the results of its analysis. The ability of an FIU to quickly share reliable financial intelligence and related information with domestic and foreign authorities is critical to the success of its mission.</td>
</tr>
</tbody>
</table>
CHAPTER SEVEN

THE FINANCIAL ACTION TASK FORCE (FATF) PROCESSES

In this chapter, the reader will learn about the Financial Action Task Force processes that are relevant to the civil society sector, and what it entails to participate in such a process as a member of the sector. By describing the concepts associated with these processes, the chapter also tries to reveal the drivers behind these processes and insights on how and why civil society ought to participate in the same.

7.1 Mutual Evaluations

The FATF- Mutual Evaluation can be defined as a peer review process, where members from different countries assess another country’s levels of implementation of the FATF Recommendations and provide an in-depth analysis of a country’s system for preventing criminal abuse of the financial system. FATF mutual evaluations reports, therefore, are a source of in-depth description and analysis of a country’s system for preventing criminal abuse of the financial system as well as, focused recommendations to the country for areas that require strengthening.\(^\text{31}\)

Mutual evaluations are strict, and a country is only deemed compliant if it can prove to the other members, that its systems are robust enough to mitigate risk related to ML/FT/PF. In other words, the onus is on the assessed country to demonstrate that it has an effective framework to protect the financial system from abuse.

7.1.1 Components of the mutual evaluation

The Mutual Evaluation Process focuses on two major components. These are effectiveness and technical compliance.

a. Effectiveness

The main component of a mutual evaluation is that of effectiveness. This entails the on-site visit to the assessed country. During this visit, the assessment team will require evidence that demonstrates that the assessed country’s measures are working and deliver the right results. What is expected from a country differs, depending on susceptibility level (s) to money laundering / terrorist financing and other associated risks. To ensure consistent and fair assessments, the assessors are guided by a detailed assessment methodology as developed by FATF.

b. Technical Compliance

Under this component of technical compliance, the assessed country is required to provide information on the laws, regulations, and any other legal instruments it has in place to combat money laundering and the financing of terrorism and proliferation.

\(^{31}\) For a 3-minute introductory video to the Mutual Evaluation Process, see for example K Karlson “The Financial Action Task Force (FATF) Mutual Evaluation Process – explained in three minutes” https://www.youtube.com/watch?v=lrA9k3uZGRk
Previously, this used to be the focus of FATF, and FATF still requires the legal framework to be in place. But experience has shown that having the laws in the books is not enough, and the focus is now on effectiveness, from ticking the box to application.

c. **The Mutual Evaluation Report**

The mutual evaluation report is, therefore, a product of an assessment of a country’s measures to combat money laundering and the financing of terrorism and proliferation of weapons of mass destruction. It includes highlights of a country’s actions to address the risks emanating from designated terrorists or terrorist organisations. The mutual evaluation report is without prejudice to the status or justification that led to the designation of an entity as a terrorist or terrorist group or organisation.

d. **The mutual evaluation processes**

---

**figure 8** - Adopted from the Financial Action Task Force, “Mutual Evaluations”
A complete mutual evaluation takes up to 18 months. The stages of this process are as follows:

i. **Assessor training.** The FATF organises regular training to train experienced national experts in the FATF Recommendations and FATF Assessment Methodology.

ii. **Country training.** The FATF organises training for representatives of the assessed country so that they know what they will need to provide and demonstrate during the process.

iii. **Selection of assessors.** The FATF selects the members of the assessment team from the pool of trained assessors.

iv. **Technical compliance.** The country provides information about its laws and regulations. The assessors analyse this information, checking if all the required laws and regulations, as required by the FATF Recommendations, are in place. Following the analysis, assessors produce a draft report, with technical compliance ratings for all 40 Recommendations as highlighted in the image below.

v. **Preliminary scoping exercise.** In preparation for the effectiveness assessment and the on-site visit, assessors undertake a preliminary scoping exercise to determine the areas of focus of the on-site visit.

vi. **On-site visit.** The assessors travel to the country for the on-site visit. Before, during and after the visit, the country needs to provide information on the effectiveness of its system in all eleven areas that are covered by the FATF Methodology.

vii. **Report drafting.** Immediately following the on-site visit, the assessors finalise the mutual evaluation report with the findings of the effectiveness and technical compliance assessment.

viii. **Plenary discussion.** The assessors present the draft report to the FATF Plenary at one of the three meetings it holds every year. The Plenary will discuss the assessors’ findings and proposed ratings.

ix. **Final quality review.** Following Plenary approval, all countries within the FATF Global Network will review the report for technical quality and consistency before it is published on the website, which is usually two months after Plenary approval.

x. **Follow-up.** After adoption, the countries are required to address the shortcomings identified in the report. All countries are subject to post-assessment monitoring, as highlighted in the image below.

### 7.1.3 Process Gaps in the Mutual Evaluation for NPOs

a. Evaluation teams, in general, may or **do not** include specialists or experts on CSOs.
b. Evaluators may or are **less knowledgeable** on issues that might affect civil society and the effectiveness of measures under R8.

c. There is often a **lack of government outreach** to civil society about the evaluation process.

d. Application of R8 in some cases has meant the **shrinking of the financial, operational, and political space for civil society in general** - counterproductive to mitigating terrorist threats.

![Figure 9 - Follow Up Stages for Implementing MER Recommendations](image)

**7.1.4 Roles of NPOs in the Mutual Evaluation Process**

**Table 6 - Opportunities for NPOs to Engage in FATF’s Mutual Evaluation Process**

<table>
<thead>
<tr>
<th>Period</th>
<th>Key Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Before the on-site visit</td>
<td>• Mobilising NPOs to participate in the process</td>
</tr>
<tr>
<td></td>
<td>• Explain the importance of NPO participation in the process</td>
</tr>
<tr>
<td>Meeting with evaluators</td>
<td>• Share the NPO perspectives of risk - with evaluators</td>
</tr>
<tr>
<td></td>
<td>• Discuss the effectiveness of current measures</td>
</tr>
<tr>
<td></td>
<td>• Discuss the effectiveness of the existing NPO self-evaluation models.</td>
</tr>
<tr>
<td>After the evaluator’s visit</td>
<td>• Participate in the FATF plenary session(s)</td>
</tr>
<tr>
<td></td>
<td>• Awareness and understanding of Recommendations from the MER</td>
</tr>
<tr>
<td></td>
<td>• Leverage on follow reports and mobilise as a collective to pushback on new restrictions affecting NPOs in the country.</td>
</tr>
</tbody>
</table>
7.2 The National Risk Assessment

Understanding the money laundering and terrorist financing, the risk is an essential part of developing and implementing a national anti-money laundering / countering the financing of terrorism (AML/CFT) regime in any jurisdiction, which includes laws, regulations, enforcement, and other measures to mitigate ML/TF risks.

A proper understanding of the ML/TF helps the county’s authority to prioritise and allocate resources efficiently. Country authorities are guided to apply AML/CFT measures in a way that ensures they are commensurate with those risks – i.e., the risk-based approach (RBA) – which is central to the FATF standards as is set out in Recommendation 1, its interpretive note (INR 1), as well as in other Recommendations (e.g., Recommendations 8, 10, 12, 26 and 28).³²

7.2.1 Stages of the National ML/TF Risk Assessment

National risk assessment is a process and can be divided into a series of activities or stages. These include identification, analysis, and evaluation. According to the FATF National Risk Assessment Guideline, the three stages are presented and briefly described below.

Table 7 - Stages of the AML/CFT National Risk Assessment

<table>
<thead>
<tr>
<th>STAGE</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identification</td>
<td>In general terms, the process of <strong>identification</strong> in the context of an ML/TF risk assessment starts by developing an initial list of potential risks or risk factors 15 countries face when combating ML/TF. These will be drawn from known or suspected threats or vulnerabilities. Ideally at this stage, the identification process should attempt to be comprehensive; however, it should also be dynamic in the sense that new or previously undetected risks identified may also be considered at any stage in the process.</td>
</tr>
<tr>
<td>Analysis</td>
<td><strong>Analysis</strong> lies at the heart of the ML/TF risk assessment process. It involves consideration of the nature, sources, likelihood and consequences of the identified risks or risk factors. Ultimately, this stage aims to gain a holistic understanding of each of the risks – as a combination of threat, vulnerabilities, and consequence to work towards assigning some sort of relative value or importance to them. Risk analysis can be undertaken with varying degrees of detail, depending on the type of risk and the purpose of the risk assessment, as well as based on the information, data, and resources available</td>
</tr>
</tbody>
</table>

**Evaluation** in the context of the ML/TF risk assessment process involves taking risks analysed during the previous stage to determine priorities for addressing them, considering the purpose established at the beginning of the assessment process. These priorities can contribute to the development of a strategy for their mitigation.

### 7.2.2 Importance of the National Risk Assessment

The results of a national risk assessment, whatever its scope, can also provide useful information to:

i. Policymakers and other authorities, for example, to formulate the national AML/CFT policies, make reasonable decisions on the legal and regulatory framework and the allocation of resources to competent authorities based on FATF Recommendation.

ii. Operational agencies, including law enforcement, other investigative authorities, financial intelligence units (FIUs), relevant border agencies, etc.

iii. Regulators, supervisors, and self-regulatory bodies (SRBs).

iv. Financial institutions, and designated non-financial businesses and professions (DNFBPs), for which the national-level ML/TF risk assessment is a critical source contributing to their ML/TF risk assessments and risk-based obligations.

v. Non-profit organisations (NPOs).

vi. AML/CFT assessors and assessment bodies more broadly, along with other international stakeholders.

vii. The public, as well as academia, specified individuals, etc.

Irrespective of the adopted approach, countries are advised to ensure that their assessment of ML/TF risk is comprehensive enough to provide an overall picture of the national ML/TF risks across the AML/CFT regime. Ideally, this picture should include sufficient breadth and depth about potential threats and vulnerabilities and their consequences to address the purpose and scope of the assessment.

### 7.2.3 Process gaps in the National Risk Assessment from the NPO perspective

**a. NPOs’ exclusion:** the assessment team, in most cases, may or do not include specialists or experts on CSOs.

**b. Limited sectoral knowledge:** the assessment team may or are less knowledgeable about issues that might affect civil society and the effectiveness of measures under R8.

**c. Willful quietness:** In some jurisdictions, there is often no information / government outreach to civil society about the process.

**d.** Application of R8 in some cases has meant the shrinking of the financial, operational, and political space for civil society in general - counterproductive to mitigating terrorist threats.
7.3 **The National Sectoral Risk Assessment for NPOs**

According to FATF and other AML/CTF standard setters, NPOs by their nature are perceived vulnerable to these crimes. For example, a non-profit organisation may be set up as a sham business to bring illegally obtained funds into the financial system. Also, legitimately obtained funds can be abused by terrorists to finance terrorist activities. This may occur when a non-profit organisation conducts fundraising activities where the contributors to the fundraising activities believe that the funds will go to relief efforts abroad, but some or all the funds are transferred to a terrorist group.

As a way of complying with **Recommendation 8**, jurisdictions are required to conduct non-profit organization sectoral ML/FT risk assessment to guide national mitigation measure for the sector. This may also play a significant role in limiting “blind and unnecessary overregulation” of the NPO sector. The World Bank and the International Monitoring Fund have developed guidelines and tools to inform national regulators to conduct a successful process.\(^3\)

### 7.3.1 FATF Typologies Report on Risk of Terrorist Abuse for NPOs

In October 2001, the Financial Action Task Force drafted eight special recommendations pertaining to terrorist financing in response to a changing threat environment that had culminated in the attacks made on September 11th of that year. Originally labelled as Special Recommendation VIII (SR VIII), the current Recommendation 8, states the following:

a. Countries should review the adequacy of laws and regulations that relate to entities that can be abused for the financing of terrorism. Non-profit organisations are particularly vulnerable, and countries should ensure that they cannot be misused:

   • by terrorist organisations posing as legitimate entities;
   • to exploit legitimate entities as conduits for terrorist financing, including for the purpose of escaping asset-freezing measures; and
   • to conceal or obscure the clandestine diversion of funds intended for legitimate purposes to terrorist organisations.

### 7.3.2 Why NPOS are at Risk of Abuse for Terrorist Financing

While non-profit organisations (NPOs), like their for-profit counterparts, face numerous risks relating to both money laundering and terrorist financing, SR VIII was designed to address specific terrorist financing vulnerabilities and threats faced by NPOs. When the 40 Recommendations were revised in 2012, the FATF integrated most of the Special Recommendations on terrorist financing into the general recommendations

---

that address both anti-money laundering (AML) activities and activities meant to counter the financing of terrorism (CFT). The FATF did, however, recognize that three Recommendations remained unique to terrorist financing and grouped them together in Section C of the Recommendations; former SRVIII, now Recommendation 8 (Measures to Prevent the Misuse of Non-profit Organisations), was one of these three. This typologies report represents a significant step forward in understanding the terrorist threat to the NPO sector. Several important findings emerged from the analysis of 102 case studies submitted by FATF member states or compiled from open sources as well as current research on the threat environment. These findings can be summarised as follows:

<table>
<thead>
<tr>
<th>Key Findings</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Key Finding 1</strong></td>
<td>The NPO sector has interconnected vulnerabilities, and terrorist entities seek to exploit more than one type of vulnerability. In the cases analysed for this project, the diversion of NPO funds by terrorist entities was a dominant method of abuse. However, other types of non-financial abuse such as the abuse of programmes, or the support for recruitment, also appeared regularly.</td>
</tr>
<tr>
<td><strong>Key Finding 2</strong></td>
<td>The NPOs most at risk appear to be those engaged in ‘service’ activities, and that operate in a proximity to an active terrorist threat. This may refer to an NPO operating in an area of conflict where there is an active terrorist threat. However, this may also refer to an NPO that operates domestically, but within a population that is actively targeted by a terrorist movement for support and cover. In both cases the key variable of risk is not geographic, but the proximity to an active threat.</td>
</tr>
<tr>
<td><strong>Key Finding 3</strong></td>
<td>Because of the nature of the threat and the resulting nature of state responses, cases of substantial risk are an important source of information for typologies analysis.</td>
</tr>
<tr>
<td><strong>Key Finding 4</strong></td>
<td>The amalgamation of many types of information held by different actors was an important factor in the detection of cases of abuse or in the identification of substantial risk.</td>
</tr>
<tr>
<td><strong>Key Finding 5</strong></td>
<td>Disruption of abuse, or the mitigation of substantial risk, was dealt with through multiple means including, but not limited to, criminal prosecution. Administrative enforcement, financial penalties, and targeted financial sanctions play important roles in disruption of abuse.</td>
</tr>
</tbody>
</table>

*Figure 10 - Key Findings of the FATF Typologies Study on the Risk of Terrorist Financing of NPOs*
### 7.3.3 What measures should countries take to protect NPOs from the risk of terrorist financing?

Countries should undertake domestic reviews of their NPO sector or have the capacity to obtain timely information on its activities, size, and other relevant features. In undertaking these assessments, countries should use all available sources of information to identify features and types of NPOs, which, by virtue of their activities or characteristics, are at risk of being misused for terrorist financing. Countries should also periodically reassess the sector by reviewing new information on the sector’s potential vulnerabilities to terrorist activities.

There is a diverse range of approaches in identifying, preventing, and combating terrorist misuse of NPOs. An effective approach, however, is one that involves all four of the following elements: (a) outreach to the sector, (b) supervision or monitoring, (c) effective investigation and information gathering and (d) effective mechanisms for international cooperation. The following measures represent specific actions that countries should take with respect to each of these elements, to protect their NPO sector from terrorist financing abuse.

<table>
<thead>
<tr>
<th>Area of Intervention</th>
<th>Measures</th>
</tr>
</thead>
</table>
| Outreach to the NPO sector concerning terrorist financing issues | i. Effective information gathering and investigation. Countries should have clear policies to promote transparency, integrity and public confidence in the administration and management of all NPOs.  
ii. Countries should encourage or undertake outreach programmes to raise awareness in the NPO sector about the vulnerabilities of NPOs to terrorist abuse and terrorist financing risks, and the measures that NPOs can take to protect themselves against such abuse.  
iii. Countries should work with the NPO sector to develop and refine best practices to address terrorist financing risks and vulnerabilities and thus protect the sector from terrorist abuse.  
iv. Countries should encourage NPOs to conduct transactions via regulated financial channels, wherever feasible, keeping in mind the varying capacities of financial sectors in different countries and in different areas of urgent charitable and humanitarian concerns. |
Supervision or monitoring of the NPO sector. Countries should take steps to promote effective supervision or monitoring of their NPO sector. In practice, countries should be able to demonstrate that the following standards apply to NPOs which account for (1) a significant portion of the financial resources under control of the sector; and (2) a substantial share of the sector’s international activities.

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>i.</td>
<td>NPOs should maintain information on: (1) the purpose and objectives of their stated activities; and (2) the identity of the person(s) who own, control, or direct their activities, including senior officers, board members and trustees. This information should be publicly available either directly from the NPO or through appropriate authorities.</td>
</tr>
<tr>
<td>ii.</td>
<td>NPOs should issue annual financial statements that provide detailed breakdowns of incomes and expenditures.</td>
</tr>
<tr>
<td>iii.</td>
<td>NPOs should be licensed or registered. This information should be available to competent authorities.</td>
</tr>
<tr>
<td>iv.</td>
<td>NPOs should have appropriate controls in place to ensure that all funds are fully accounted for and are spent in a manner that is consistent with the purpose and objectives of the NPO’s stated activities.</td>
</tr>
<tr>
<td>v.</td>
<td>NPOs should follow a “know your beneficiaries and associate NPOs” rule, which means that the NPO should make best efforts to confirm the identity, credentials, and good standing of their beneficiaries and associate NPOs. NPOs should also undertake best efforts to document the identity of their significant donors and to respect donor confidentiality.</td>
</tr>
<tr>
<td>vi.</td>
<td>NPOs should maintain, for a period of at least five years, records of domestic and international transactions that are sufficiently detailed to verify that funds have been spent in a manner consistent with the purpose and objectives of the organisation and should make these available to competent authorities upon appropriate authority. This also applies to information mentioned in paragraphs (i) and (ii) above.</td>
</tr>
<tr>
<td>vii.</td>
<td>Appropriate authorities should monitor the compliance of NPOs with the requirements of this Recommendation. Appropriate authorities should be able to apply effective, proportionate, and dissuasive sanctions for violations by NPOs or persons acting on behalf of these NPOs.</td>
</tr>
</tbody>
</table>
### Effective information gathering and investigation

| i. | Countries should ensure effective cooperation, coordination, and information-sharing to the extent possible among all levels of appropriate authorities or organisations that hold relevant information on NPOs. |
| ii. | Countries should have investigative expertise and capability to examine those NPOs suspected of either being exploited by, or actively supporting, terrorist activity or terrorist organisations. |
| iii. | Countries should ensure that full access to information on the administration and management of a particular NPO (including financial and programmatic information) may be obtained during an investigation. |
| iv. | Countries should establish appropriate mechanisms to ensure that, when there is suspicion or reasonable grounds to suspect that a particular NPO: (1) is a front for fundraising by a terrorist organisation; (2) is being exploited as a conduit for terrorist financing, including for the purpose of escaping asset freezing measures; or (3) is concealing or obscuring the clandestine diversion of funds intended for legitimate purposes, but redirected for the benefit of terrorists or terrorist organisations, this information is promptly shared with relevant competent authorities, in order to take preventive or investigative action. |

### Effective capacity to respond to international requests for information about an NPO of concern consistent with Recommendations on international cooperation, countries should identify appropriate points of contact and procedures to respond to international requests for information regarding NPOs suspected of terrorist financing or other forms of terrorist support.
## Chapter Eight

### Effective Strategies to Protect the NPO Sector from Vulnerability to Terrorist Financing

#### 8.1 Building an Effective Self-Regulation Program

NPOs can maintain an effective self-regulation program by identifying red flags for to build an effective AML/CFT compliance practices through acting in five areas in the following ways:

<table>
<thead>
<tr>
<th>Area of Focus</th>
<th>Key Actions</th>
</tr>
</thead>
</table>
| **Organizational Level** | • Where donations are conditional on being used in partnership with individuals or organizations where the NPO has concerns about those individuals or organizations  
• Where an NPO is asked to provide services or benefits on favourable terms to the donor or a person nominated by the donor  
• Unusual or substantial one-time donations are received from unidentifiable or suspicious sources.  
• If a series of small donations are received from sources that cannot be identified or checked  
• Where donations are made in a foreign currency or foreign sources where financial regulation or legal framework is not as rigorous  
• If conditions attached to a donation are as such that NPO would merely be a vehicle for transferring funds from one individual or organization to another individual or organization  
• Where payments received from a known donor but through an unknown party  
• Where donations are received from unknown or anonymous bodies  
• Where payments received from an unusual payment mechanism where this would not be a typical method of payment |
| **Beneficiaries** | • Where there may appear signs that people may have been placed on distribution and aid lists by providing kickbacks and bribes to officials  
• Lists of beneficiaries contain multiple manual corrections, multiple names may appear, may contain more family members  
• Evidence that third parties or intermediaries have demanded payment for recommending or nominating beneficiaries  
• Where an NPO aids, services or support based on a certain sum of money per beneficiary and the numbers are relatively high  
• Where an NPO provides services to larger numbers of beneficiaries, where it may be easier to disguise additional beneficiaries  
• Fake or suspicious identity documents  
• Beneficiaries with identical characteristics and addresses or multiple identical or similar names and signatures |
| Employees | • Indications that staff may be living beyond their means or appearing at unusual times  
• Staff carrying out tasks or jobs they should not be, or other unusual staff behavior or conduct  
• Sudden or increased staffing costs |
| --- | --- |
| Projects | • Invoices and paperwork have been tampered with, altered in crucial aspects with handwritten amendments  
• Inventory shortages  
• The project is vague or lacks adequate financial or technical details  
• Missing key documents or only copies can be reproduced  
• Lack of evidence to show fair and transparent tendering or procurement procedures  
• Invoices and papers recording a higher cost for goods or services than expected or agreed  
• Signatures confirming receipt or payments are missing, or the invoice unsigned or undated  
• Receipts have been signed and dated a long time after the goods or services should have been delivered  
• Repeated excuses of system crashing, losing records or paperwork  
• Discrepancies between budgeted needs and payments requested  
• Requests for payments in cash to be made to an unknown third party or other organization  
• Funds are not being banked or accounted for  
• Emails from new or unusual email addresses not in the partner’s domain name or from someone who is not a previously agreed contact point  
• Inconsistencies between narrative reports and financial claims and reports |
| Partners | • The structure or nature of the proposed project makes it difficult to identify the partner and verify their identity and details  
• The proposal includes delegating work to other unknown partners or newly formed organizations  
• Partners request unnecessary or unusual levels of privacy and secrecy  
• Requests by partners to use a particular auditor or accountant  
• The project involves unusual payment mechanisms, requests for cash, or for money to be paid into an account not held in the name of the partner, or in a country in which the partner is not based and not where the project is being carried out |

8.2 Building Effective AML/CFT Compliance Practices

NPOs are defined by their purpose, their reliance on contributions from donors and the trust placed in them by the wider community. Not all NPOs are inherently high-risk organizations, and it is desirable to identify the high-risk NPOs, i.e., NPOs which by their activities, characteristics, asset size, international and geographical activities are likely
to be at risk for terrorist financing abuse, for proper risk management.
NPOs should perform and maintain the regular performance of compliance tests to examine the effectiveness of AML/CTF systems and controls implemented by the NPO. Findings must be documented, and recommendations provided purposed at rectification of any deficiencies identified. However, for a shift to an enhanced AML/CFT control system, an organization may consider the following:

<table>
<thead>
<tr>
<th>Area of Focus</th>
<th>Key Actions</th>
</tr>
</thead>
</table>
| Day to Day Measures | • Observe appropriate internal governance and financial controls and ensure that all finances are fully accounted for and are spent in a manner that is consistent with the purpose of the organization (NPO). The appropriateness of the AML/CFT control measures is dependent on the risks level and the NPO.  
• Maintain proper and adequate financial records for both the receipt and use of all financial resources together with audit trails of decisions made. Records of both domestic and international transactions must be sufficiently detailed to verify that funds have been appropriately spent as intended and, in a manner, consistent with the purpose and objectives of the organization.  
• Ascertained what due diligence, monitoring and verification of the use of funds they need to carry out to meet their legal duties as per the AML/CFT obligation.  
• Take reasonable and appropriate steps to know who your beneficiaries are, at least in broad terms, conduct appropriate verification where the risks are high and have clear beneficiary selection criterion, which is consistently applied |
| Know Your Donors   | • Before receiving any donor funds, NPOs should establish that the donor is not placed on the United Nations' list of persons who are linked to terrorist financing or against whom a ban, sanction or embargo subsists.  
• NPOs should conduct, on a risk-based approach, a reasonable search of public information, including information available on the Internet, to determine whether the donor or their key employees, board members or other senior managerial staff are suspected (or not) of being involved in activities relating to terrorism, including terrorist financing.  
• NPOs must undertake best efforts to document the identity of their significant donors. NPO must collect, verify, and maintain a record of correct and complete identification particulars of substantial donors. |
| Know Your Beneficiaries and Partners (KYB/P) | • NPO must ascertain correct and complete identification particulars of each of its beneficiary (person, group of persons or organization, etc.) who receives cash or services or in-kind contributions.  
• In cases where the projects are implemented through partnership agreements with other partners, the NPO shall make it a part of its project agreements that partners shall maintain and share beneficiaries’ information.  
• NPOs must ensure that the partner organizations shall not be from any such organization whose license has been revoked or registration cancelled by other authorities.  
• In case the beneficiary is an organization/group of persons, the donor NPO must know a detailed profile and particulars of such an organization. The NPO shall ensure that its beneficiaries are not linked with any suspected terrorist activity or any link with terrorist support networks. |
| Know your Employees/Staff/Volunteers (KYE/S/V) | • An NPO must maintain records of particulars of its employees (both nationals and foreign), including but not limited to a permanent address, present address, copy of National ID Card, passport number, nationality, personal email ID, phone or mobile number, experience, etc. |
According to FATF Recommendation 8, governments are required to review and assess the “adequacy of laws and regulations that relate to non-profit organizations and develop commensurate measures to mitigate any risk and threat posed to the sector.” The FATF makes emphasis on the application of a risk-based approach as opposed to a broad-brush approach to countries’ terrorist financing measures. To FATF, countries should avoid the imposition of blanket restrictions on the nonprofit sector, and justify their regulations based on evidence of existing risk. Besides, the FATF expects that countries should update their risk assessments periodically, recognizing that risk changes over time and in different sectors. A meaningful way that governments should assess risk in the nonprofit sector is through continuous dialogue and consultation with civil society stakeholders - you!

All counter-terrorist financing and anti-money laundering regulation of nonprofits in a particular country should be based on the risk assessment, so NPOs must participate in this effort. The Global NPO Coalition on FATF provides tools and wealth of knowledge with a detailed explanation of how NPO can participate in these processes as stakeholders as enlisted below.

## 9.1 Conducting Non-Profit Organization Tailored Outreach

<table>
<thead>
<tr>
<th>Key Actions</th>
<th>Best Practices</th>
</tr>
</thead>
<tbody>
<tr>
<td>Conduct relevant outreach (dialogue, organize awareness workshops) with stakeholders including NPOs, government, financial institutions, regulators, and regional/international bodies.</td>
<td>• Roundtables with relevant government ministries, departments, and agencies (MDAs)</td>
</tr>
<tr>
<td></td>
<td>• Developing and cultivating relationships with key regulatory actors for the NPO sector</td>
</tr>
<tr>
<td></td>
<td>• Continuous engagement on emerging issues</td>
</tr>
</tbody>
</table>

34 For additional insights on outreach engagements, see the Global NPO Coalition on FATF at https://fatfplatform.org/get-involved/conducting-relevant-outreach...
9.2 Perform NPO focused Mutual Monitoring.

<table>
<thead>
<tr>
<th>Key Actions</th>
<th>Best Practices</th>
</tr>
</thead>
<tbody>
<tr>
<td>While the government monitors the NON-PROFIT ORGANISATION sector for potential terrorism financing risk and sets out rules on accountability and transparency, the NPO sector needs to monitor the measures imposed to ensure that they are proportionate to the risk and do not hamper legitimate charitable activity in any way.(^\text{35})</td>
<td>• Establishing national NPO working groups&lt;br&gt;• Designing and facilitating initiatives for regular monitoring of regulatory implications.&lt;br&gt;• Publishing policy briefs targeting key stakeholders.</td>
</tr>
</tbody>
</table>

9.3 Engaging in the National Risk Assessment Process

<table>
<thead>
<tr>
<th>Key Actions</th>
<th>Best Practices</th>
</tr>
</thead>
<tbody>
<tr>
<td>The NPO sector would be at the table when the government is determining whether the industry is at risk of being abused for terrorism financing.(^\text{36})</td>
<td>• Conducting shadow risk assessments&lt;br&gt;• Advocate for the amendment or repealing of legislation shrinking civic space&lt;br&gt;• Understand the recommendations from the NRA&lt;br&gt;• Develop strategies for monitoring the state’s implementation of recommendations</td>
</tr>
</tbody>
</table>

35 For additional insights on outreach engagements, see the Global NPO Coalition on FATF at https://fatfplatform.org/get-involved/mutual-monitoring/

36 For additional insights on outreach engagements, see the Global NPO Coalition on FATF at https://fatfplatform.org/get-involved/engaging-in-risk-assessment/ Also, Nigeria published a National Risk Assessment for TF and ML (completed in 2016), which identified Designated Non-Financial Businesses and Institutions (DNFIs), of which NON-PROFIT ORGANISATIONS are a subset, as being amongst those sectors most vulnerable to ML/TF. Spaces for Change, a Global NON-PROFIT ORGANISATION Coalition member, challenged (2019) this assessment of risk for the non-profit sector, disputing the official classification of NON-PROFIT ORGANISATIONS as DNFIs and teasing out the nuances between vulnerability and threat, among other issues. The report led to increased and constructive engagement with the FIU (SCUML) and other government and NPOs stakeholders, including GIABA, the FATF-Style Regional Body for West Africa.
## 9.4 Engaging in the Mutual Evaluation Process

<table>
<thead>
<tr>
<th>Key Actions</th>
<th>Best Practices</th>
</tr>
</thead>
<tbody>
<tr>
<td>NPO Participation and Engagement in</td>
<td>Find out who represents your government at the FATF plenary (likely to be the Ministry of Finance) and request a meeting.</td>
</tr>
<tr>
<td>the Mutual Evaluation Process.37</td>
<td>If your country is not a member of FATF find out who in government is the contact for the FATF regional body. A list of FATF members and regional bodies is here.</td>
</tr>
<tr>
<td></td>
<td>Be aware of when your Country is up for a FATF evaluation. Form a coalition to advocate the cause of a free and fully functioning civil society space.</td>
</tr>
<tr>
<td></td>
<td>Learn from civil society in countries that have gone through the mutual evaluation process.</td>
</tr>
<tr>
<td></td>
<td>Keep tabs on and highlight rules/regulations/laws that are, either directly or indirectly, affecting your ability to function effectively.</td>
</tr>
</tbody>
</table>

## 9.5 Gathering Evidence and Information

<table>
<thead>
<tr>
<th>Key Actions</th>
<th>Best Practices</th>
</tr>
</thead>
<tbody>
<tr>
<td>Documentation, monitoring and</td>
<td>Gather evidence and information on the unintended consequences of countering the financing of terrorism (CFT) agenda on the operational environment of civil</td>
</tr>
<tr>
<td>tracking incidents of possible and</td>
<td>society in your Country, whether that is banks blocking transactions to conflict zones or closing NPO accounts; laws being enacted to restrict foreign funding;</td>
</tr>
<tr>
<td>actual misapplication of R8</td>
<td>the introduction of burdensome governance and audit requirements; the prosecution of human rights defenders; or limitations to the right to assemble or protest.38</td>
</tr>
</tbody>
</table>

---


38 Civicus’ Enabling Environment Index (EEI) examines conditions within which civil society work. It ranks the governance, socio-cultural and socio-economic environments for civil society in 109 countries. CIVICUS also publishes an annual State of Civil Society Report.
### 9.6 Raising NPO Awareness

<table>
<thead>
<tr>
<th>Key Actions</th>
<th>Best Practices</th>
</tr>
</thead>
</table>
| Empower local NPOs with knowledge on existing FATF style legislation and its implications on civic space in the country to develop effective advocacy strategies. | Form a NON-PROFIT ORGANISATION coalition on FATF to advocate for a free and fully functioning civil society.  
Keep tabs on and highlight rules/regulations/laws that are, either directly or indirectly, affecting your ability to function effectively.  
Be aware of when your Country is up for a FATF evaluation. Engage in the process to the extent possible. Learn from civil society in countries that have gone through the Mutual Evaluation process.  
Join the Global NON-PROFIT ORGANISATION Coalition on FATF for guidance, best practice examples and engagement and advocacy strategies.  
Collate and disseminate already-existing rules/regulations/laws on CFT/CT, already-existing sectoral self-regulation measures and their effectiveness; the adverse impact of any new/already-existing AML/CFT rules/regulations/laws; examples of shrinking civic space in the Country. |

### 9.8 Perform sector-led risk assessments for NPOs

<table>
<thead>
<tr>
<th>Key Actions</th>
<th>Best Practices</th>
</tr>
</thead>
</table>
| Empower local NPOs with knowledge on existing FATF style legislation and its implications on civic space in the country to develop effective advocacy strategies. | Setting up National Risk Assessment Working Groups  
Design and implement a risk a three-pronged risk assessment.  
Present risk assessment results in a multi-stakeholder platform  
develop a detailed action plan that addresses the AML/CFT risks. The implementation of the action plan must follow a risk-based approach. |

---

39 Preparation (It entails activities related to setting up the working group that is to perform the task. At this stage, the following elements must be answered: Who constitutes the group and why? What level of knowledge should a group member have? Which tool is the group going to use? Do group members have knowledge of the tool and who they are to target?); Assessment (This also begins with a 3-4 days’ workshop for all Working Group members who are committed to the process. The aim of this workshop is to equip the group members with necessary hands-on knowledge and skills on the administration of the assessment tool and unveiling the assessment process. The workshop should include a reflection session on the money laundering and terrorist financing risks dynamics in the in the sector and the country. During this stage, the Working Group is expected to develop a “SMART” roadmap that runs the process through to completion. DPI has a technical team to guide members of the NPO sector throughout this stage); Finalisation (Evaluating the risk assessment and the results therein, 2 Analysis of the proposed risk-based action plans, Implementation model of the plan and any other issue related to the same.)
BASIC UNDERSTANDING OF AML/CFT ISSUES FOR NON-PROFIT ORGANISATIONS

As the operating space for civil society becomes increasingly small, elections also pose a heightened period of danger for HRDs. Regressive legislation has been introduced in many nations, limiting people’s rights to free speech and peaceful assembly. Counter-terrorism laws are continually being misused to target the legitimate work of defenders of human rights. With broad and ambiguous language, NGO and Media Bills are increasingly being passed, promoting judicial prosecutions under the guise of ‘threatening national security’ against independent human rights organizations and media outlets. Administrative and bureaucratic abuse is used throughout the country to undermine defenders’ work of human rights and journalists.

Generally, collective analysis of the AML/CFT architecture highlighted above reveals two broader concerns. Firstly, the anti-money laundering legislation contains general and overarching provisions under which the assets and business transactions of persons and organizations of interest may be closely monitored and curtailed under the guise of public interest. Secondly, Anti-terrorism legislation contains several broad provisions that leave it open to abuse. These include such general offences as the ‘promotion of terrorism’ that may catch a wide range of legitimate activities within its ambit, especially in the areas of human rights advocacy.

10.1 Key NPO concerns with AML Regulations in Africa

Key NPO Concerns with CF Legislation In Africa Concerning Counter-terrorism legislation, the following key issues arise from a closer look at the legislation of various countries:

<table>
<thead>
<tr>
<th>Issue</th>
<th>Key NPO concerns</th>
</tr>
</thead>
<tbody>
<tr>
<td>Broad and vague definitions of terrorism</td>
<td>The definition of terrorism is mostly broad and vague. Therefore, it could be subjectively interpreted to undermine fundamental rights guaranteed under various constitutions, including freedom of expression, freedom of assembly, and association.</td>
</tr>
<tr>
<td>Possible misuse of ‘aiding and abetting’ provisions</td>
<td>Provisions on aiding and abetting terrorism are mainly broad and could be subjectively interpreted to restrict fundamental rights guaranteed under the constitution.</td>
</tr>
<tr>
<td>Absence of judicial oversight in CFT legislation</td>
<td>In most cases, the absence of judicial oversight creates an opportunity for the broad interpretation and misuse of the powers, resulting in the violation of organizations’ right to privacy and individuals operating non-profit activities</td>
</tr>
</tbody>
</table>
Increased securitization of law enforcement

Definitions of terrorism in most CFT legislation that lack precision enable authorities to apply them arbitrarily or discriminatorily. This could lead to the criminalization of otherwise peaceful activities in the pursuance of the legitimate exercise of fundamental freedoms, such as freedom of expression.

10.2 What key actions can NPOs and Regulators take?

a. Non-Profit Organizations

<table>
<thead>
<tr>
<th>Actions</th>
<th>Areas of Intervention</th>
</tr>
</thead>
<tbody>
<tr>
<td>Raising awareness</td>
<td>Actors in the Civil society must find creative ways to raise awareness about the challenges faced because of the global security framework. These may include but not limited to:</td>
</tr>
<tr>
<td>Scaling up regional and international engagement</td>
<td>Broaden, deepen, and sustain the sector’s engagement with the global AML/CFT architecture, including FATF, UN agencies and bodies that are traditionally seen as dealing with security-related issues both at the international and national level.</td>
</tr>
<tr>
<td>Developing and cultivating common ground with national regulators.</td>
<td>The sector ought to explore innovative ways aimed at identifying entry points at the national level for oversight and accountability purposes.</td>
</tr>
<tr>
<td>Trend Analysis</td>
<td>Maintaining a robust trend analysis program should be deliberate, to inform quality engagements, relevant awareness-raising and constructive AML/CTF process participation.</td>
</tr>
</tbody>
</table>

b. Regulators

<table>
<thead>
<tr>
<th>Actions</th>
<th>Areas of intervention</th>
</tr>
</thead>
<tbody>
<tr>
<td>Facilitating Independent oversight</td>
<td>States should establish an independent mechanism to review and oversee the exercise of emergency powers, terrorism legislation, administrative measures related to terrorism, and legislation addressing ML/FT. The mandates of such independent mechanisms should specifically include the effects of such legal measures on the functioning and capacity of civil society</td>
</tr>
<tr>
<td>Promote clear definitions of terrorism</td>
<td>Governments should also ensure that the definitions of ML/FT in national laws must not be overly broad and vague. They must be precise and sufficiently clear to avoid including members of civil society, or non-violent acts carried out in the exercise of fundamental freedoms. The protection of national security must be narrowly construed. Emergency measures must be strictly limited, and not be used to crack down on civil society actors and stifle freedom of expression.</td>
</tr>
<tr>
<td>Ensure an enabling environment for NPOs to access resources</td>
<td>Measures that aim to regulate the existence and control and limit the funding of civil society must comply with the requirements of proportionality, necessity, and non-discrimination. The failure to comply with administrative requirements must never be criminalized.</td>
</tr>
</tbody>
</table>
Glossary

A

Anti-money laundering program
A developed program designed to assist institutions in their fight against money laundering and terrorist financing.

Arrest warrant
An order by court authorizing a law enforcement officer to seize and detain a particular person and require him or her to provide an answer to a complaint or otherwise appear in court.

B

Bank secrecy
This refers to laws/guidelines/protocols for institutions or jurisdictions that prohibit banks from revealing information about an account—or even disclosing its existence—without the consent of the account holder.

Beneficiary
This refers to natural or legal who benefits from a transaction, such as a party receiving the proceeds of a wire, a payout on an insurance policy.

C

Cash-intensive business
It is any kind of business in which customers usually pay with cash for the products or services provided, such as restaurants, pizza delivery services, taxi firms, coin-operated machines or car washes.

Confidentiality
Simply defined as keeping information that is classified ad confidential out of public or unauthorized view.

Confiscation
This includes forfeiture where applicable and refers to the permanent deprivation of funds or other assets by order of a competent authority or a court.

Corporate vehicles
Refers to legal entities that may be vulnerable to abuse/misuse such as private limited companies and public limited companies whose shares are not traded on a stock exchange, trusts, non-profit organizations, limited partnerships and limited liability partnerships and private investment companies.
**Correspondent banking**
A type of banking services provided by one bank (the correspondent bank) to another bank (the respondent bank).

**Criminal proceeds**
Any property derived from or obtained, directly or indirectly, through the commission of a crime.

**Currency smuggling**
The illegal movement of large quantities of cash across borders.

**Customer due diligence (CDD)**
Refers to Anti-money laundering controls measures and procedures that enable a financial institution to predict with comparative certainty the types of transactions in which the customer is likely to engage.

**D**

**Designated non-financial businesses and professions.**
FATF recommends specific standards apply to non-financial businesses and professions, including specifically casinos, real estate agents; dealers in precious metals and precious stones; lawyers, notaries, other independent legal professionals and accountants and trust and company service providers who prepare or carry out certain duties on behalf of their clients.

**E**

**Electronic funds transfer (EFT)**
Refers to the movement of funds between financial institutions electronically.

**Electronic money (e-money)**
This comprises a series of monetary value units in some electronic format, such as being stored electronically online, on the hard drive of a device or the microchip of a plastic card.

**Enhanced due diligence (EDD)**
Building on customer due-diligence, EDD involves a call for additional measures aimed at identifying and mitigating the risk posed by higher-risk customers.

**Extradition**
Handing over of an accused or convicted person by one jurisdiction to another under an agreement that specifies the terms of such exchanges.

**Extraterritorial reach**
The influence of one country’s laws and policies to the citizens and institutions of another.
Financial Action Task Force (FATF)

FATF is an inter-governmental body that was established in 1989 by the Group of Seven industrial nations to foster the creation of national and global measures to combat money laundering. In 2012, FATF substantially revised its 40 + 9 Recommendations and reduced them to 40. See www.fatf-gafi.org.

Freeze

To prevent or restrict the exchange, withdrawal, liquidation or use of assets or bank accounts.

Integration

The integration phase often referred to as the third and last stage of the classic money laundering process; places laundered funds back into the economy by re-entering the funds into the financial system and giving them the appearance of legitimacy.

Knowledge

Mental state accompanying a prohibited act. According to the FATF, The Interpretive Notes to Recommendation 3 of the FATF 40 Recommendations of 2012 say that countries should ensure that the intent and knowledge required to prove the offence of money laundering is consistent with the standards outlined in the Vienna and Palermo Conventions, including the concept that such a mental state may be inferred from objective factual circumstances. Knowledge can be deemed, under certain circumstances, to include willful blindness; that is “the deliberate avoidance of knowledge of the facts,” as some courts have defined the term.

Know your beneficiaries (KYB)

Anti-money laundering policies and procedures for acquiring a better knowledge and understanding of the primary and secondary beneficiaries of the organization programs to detect conflicts of interests, money laundering, past criminal activity and suspicious activity.

Know your customer (KYC)

Anti-money laundering policies and procedures used to determine the true identity of a customer and the type of activity that is normal and expected, and to detect activity that is unusual for a particular customer.

Know your donor (KYD)

Anti-money laundering policies and procedures for acquiring a better knowledge and understanding of the donor by a granter for detecting conflicts of interests, money laundering, past criminal activity and suspicious activity.
Know your employee (KYE)
Anti-money laundering policies and procedures for acquiring a better knowledge and understanding of the employees of an institution to detect conflicts of interests, money laundering, past criminal activity and suspicious activity.

Layering
It is the second phase of the three-step money laundering process. It does involve creating complex levels of financial transactions designed to disguise the audit trail and to provide no trace of the illicit gains from the illegal source.

Memorandum of understanding (MOU)
An agreement between two parties establishing a set of principles that govern their relationship on a particular matter.

Money laundering
The process of disguising the existence, source, movement, destination or illegal application of illicitly derived property or funds to make them appear legitimate.

Money laundering reporting officer (MLRO)
Refers to the person responsible for overseeing an institution’s anti-money laundering activities and program and for filing reports of suspicious transactions with the national FIU.

Monitoring
A continuous process that monitors the transactions of customer activity that seem unusual or suspicious patterns, trends or outlying transactions that do not fit a normal pattern.

Non-governmental organization (NGO)
NGOs can be defined as those organizations not for profit gains, established to perform a variety of service and humanitarian functions, including bringing citizen concerns to governments, advocating for causes and encouraging political participation.

Non-profit organizations (NPO)
These can take on a variety of forms, depending on the jurisdiction and legal system, including associations, foundations, fund-raising committees, community service organizations, corporations of public interest, limited companies and benevolent public institutions.
Operational risk
Means a direct or indirect loss of operations due to inadequate or failed internal processes, people or systems, or as a result of external events.

Placement
This is the first phase of the classical three stages of money laundering process: The physical disposal of proceeds derived from illegal activity.

Politically exposed person (PEP)
According to FATF, a PEP is an individual who has been entrusted with prominent public functions in a foreign country, such as a head of state, senior politician, senior government official, judicial or military official, a senior executive of a state-owned corporation or essential political party official, as well as their families and close associates. The term PEP does not extend to middle-ranking individuals in the specified categories.

Predicate crimes
Refers to a list of unlawful activities whose proceeds, if involved in the subject transaction, can give rise to prosecution for money laundering. Predicate crimes are sometimes defined as felonies or “all offences in the criminal code.”

Red flag
A caution signal that should bring attention to a potentially suspicious situation, transaction or activity.

Regulatory agency
Refers to a government entity responsible for supervising and overseeing one or more categories of financial institutions and accounting persons. The agency generally has authority to issue regulations, to conduct examinations, to impose fines and penalties, to curtail activities and, sometimes, to terminate charters of institutions under its jurisdiction. Most financial regulatory agencies play a significant role in preventing and detecting money laundering and other financial crimes.

Reputational risk
The potential that adverse publicity regarding a financial institution’s business practices and associations, whether accurate or not, will cause a loss of confidence in the integrity of the institution.

Respondent bank
A bank for which another financial institution establishes, maintains, administers or
manages a correspondent account.

**Risk-based approach**

According to FATF recommendation 1, the assessment of the varying risks associated with different types of businesses, clients, accounts and transactions to maximize the effectiveness of an anti-money laundering program.

**S**

**Seize**

Refers to the action of that prohibits the transfer, conversion, disposition or movement of funds or other assets based on a measure initiated by a competent authority or a court under a freezing mechanism. Unlike a freeze, a seizure allows the competent authority to take control of specified funds or other assets.

**Shell bank**

Bank that exists on paper only and that has no physical presence in the country where it is incorporated or licensed, and which is unaffiliated with a regulated financial services group that is subject to adequate consolidated supervision.

**Smurfing**

The use of multiple individuals and multiple transactions for making cash deposits, buying monetary instruments or bank drafts in amounts under the reporting threshold.

**Structuring**

Refers to an Illegal act of dividing cash deposits or withdrawals into smaller amounts, or purchasing monetary instruments, to stay under a currency reporting threshold.

**Subpoena**

Compulsory legal process issued by a court to compel the appearance of a witness at a judicial proceeding, sometimes requiring the witness to bring specified documents.

**Suspicious activity**

A questionable customer behaviour or activity that may be linked to a money laundering or other criminal offence, or the financing of terrorist activity.

**Suspicious transaction report (STR)**

A mandatory filing required by reporting entities that include a financial institution’s account of a questionable transaction.

**T**

**Tipping off**

An illegal act of notifying a suspect that he or she is being investigated or pursued by
the authorities.

**U**

**United Nations (U.N.)**

An international organization that was established in 1945 by 51 countries committed to preserving peace through cooperation and collective security.


Adopted in 2001, the resolution requires member nations to take a series of actions to combat terrorism through the adoption of laws and regulations and the establishment of administrative structures.

**V**

**Virtual currency**

A medium of exchange that operates in the digital space that can typically be converted into either a fiat (e.g., government-issued currency) or it can be a substitute for real currency.

**W**

**Willful blindness**

Refers to a “deliberate avoidance of knowledge of the facts” or “purposeful indifference.”

*Source:* Majorly adapted from the Association of Certified Anti-Money Laundering Specialists (ACAMS) study guide for ACAMS certification exam