REPUBLIC OF KENYA

TERRORISM FINANCING NATIONAL RISK ASSESSMENT GUIDANCE

February - 2025


National Terrorism Financing Threat
Islamic States in Iran and The Levant
The major ISIL faction affecting Kenya is based in Somalia
Al Shabaab
The major terrorist organisation impacting Kenya
Islamic State Central Africa Province
This is the ISIL faction in DRC
Islamic State Faction in Mozambique
IKnown as Ahlu Sunna wal-Jama'a
Oromo Liberation Front/ Oromo Liberation Army
Cross-border organised criminal group in Ethiopia which is linked to Al Shabaab
Domestic Organised Criminal Groups
Have no link with TF but are vulnerable for TF abuse.

PURPOSE AND APPLICATION OF THE GUIDANCE

Between 2023 and 2024, Kenya conducted the following terrorism (TF) related risk assessments: Terrorism financing national risk assessment, non-profit organizations (NPOs) terrorism financing risk assessment, virtual assets (VAs) and virtual assets service providers (VASPs) risk assessment, legal persons and legal arrangements risk assessment, Central Bank of Kenya licensees' sectoral risk assessments, tax crimes risk assessment and Capital Markets Authority licensees' risk assessments. The assessments were intended to improve the understanding of ML risks in the country.

However, these risk assessments were conducted simultaneously by distinct teams using different approaches. As such, the outcomes and recommendations were apparently not harmonized to seamlessly guide mitigation process in the country. This Guidance is therefore, necessary to ensure consistent communication of the results from the TF risk assessments so that the users, implementers and members of the public are enabled to have clear understanding of the outcomes and context of the TF risks in the country.

The objective of the TF Risk Assessment Guidance, 2025 is therefore, to provide a concise document for seamless countering terrorism financing (CFT) outreach, sensitization and creation of awareness for all the categories of the reporting institutions, supervisory and regulatory bodies, law enforcement as well as competent authorities. In this regard, whilst the Guidance is a summary document, the content still has sufficient detail for the target audience to understand the TF risk profile for Kenya.

ENFORCEABILITY OF THE GUIDANCE

The Guidance shall be enforced in line with the following provisions of regulation *20(2), (3)* and *(4)* of the Proceeds of Crime and Anti-Money Laundering Regulations, 2023: -

2) *Where higher risks are identified, either at national, sectoral or institutional level, a reporting institution shall address such risks through—*
   a) *applying enhanced measures to manage and mitigate the identified risks; or*
   b) *ensure that this information is incorporated into its risk assessments.*

3) *Where it is determined that a beneficiary who is a legal person or a legal arrangement presents a higher risk, a reporting institution shall take enhanced measures including taking reasonable measures to identify and verify the identity of the beneficial owner of the beneficiary, at the time of payout.*

4) *A reporting institution shall perform enhanced due diligence where the money laundering and terrorism financing risks are higher.*

FOREWORD

The February 2024 Post-Observation Period Report (POPR) for Kenya covered September 2022 – October 2023. This followed publication of the second Mutual Evaluation Report (MER) for Kenya by the Eastern and Southern Africa Anti-Money Laundering Group (ESAAMLG) in September 2022. During this period, the country doubled its effort to address the Recommendations of the MER. Key among them was the need to broaden the understanding of money laundering and terrorism financing (ML/TF) risks facing the country by incorporating salient risk elements, factors and sectors, including those relating to virtual assets, legal structures, legal arrangements, among others, in the ML/TF national risk assessments.

In this regard, and in order to improve the understanding of ML/TF risks in the country at both national and sectoral levels as recommended by the MER, the country conducted the following TF-related risk assessments:- the terrorism financing national risk assessment, virtual assets (VAs) and virtual assets service providers (VASPs) risk assessment, legal persons and legal arrangements risk assessment, Central Bank of Kenya licensees' sectoral risk assessments, non-profit organizations (NPOs) risk assessment and Capital Markets Authority licensees' risk assessment.

The responsible FATF's Joint Review Group verdict on the 2024 POPR was that Kenya conducted a number of risk assessments, both at the national and sectoral levels, simultaneously in 2023. As such, the outcomes and recommendations of the risk assessments were apparently not harmonized to seamlessly guide mitigation process in the country. This observation could have resulted from the fact that the risk assessments were conducted by distinct working groups who possibly faced limited time to cross-check and effectively reconcile the outcomes.

Consequently, and as part of the International Corporation Review Group (ICRG) follow-up process, Kenya agreed to implement a 15 Item Action Plan (replete with sub-items) with the FATF. Among these, Item 2 require Kenya to; "*Produce guidance compiling and presenting the results of the NRA and other risk assessments in a consistent manner and, using this guidance, conduct sensitization activities for competent authorities and the private sector*".

To improve the combating terrorism financing (CFT) landscape in the country and to fully address the prevailing Action Items under the ICRG process, it is necessary to ensure that the results and recommendations of all the terrorism financing related risk assessments are communicated in a consistent manner. The objective is to also ensure that the implementers of risk outcomes and members of the public have a clear understanding of the findings and context of TF risks in the country. Timeous implementation of Item 2 of the Kenya's Action Plan with FATF is also crucial to enable Kenya exit the ICRG increased monitoring and follow-up process.

Based on the foregoing, Kenya has developed this Terrorism Financing National Risk Assessment Guidance, 2025 by drawing together the summaries of all the TF-related risk assessments conducted at both sectoral and national levels. Specifically, this guidance document sought to harmonize all the TF-related risk assessments by ensuring consistencies in the flow, language, results and recommendations, in line with the National Counter-Financing of Terrorism Strategy, 2024-2027.

I would like to express my gratitude to the Counter Financing of Terrorism Inter- Ministerial Committee (CFTIMC), which is chaired by the Cabinet Secretary for the Ministry on Interior and National Administration, for the steady CFT policy guidance. The CFTIMC is the coordinating authority to implement UN Security Council Resolutions relating to the suppression of the financing of terrorism and proliferation of weapons of mass destruction in the country. The Committee is also charged with the mandate of formulation and supervision of the implementation of the National Strategy and Action Plan on Counter Financing of Terrorism. I also thank the National Task Force to Combat Money Laundering, Terrorism and Proliferation Financing (NTF) for the conducive forum as well as platform for AML/CFT/CPF dialogue and information sharing.

I would also like to thank the World Bank and other development partners for availing the risk assessment tools and methodologies for our use. Finally, I thank the Risk Assessments Consolidation Working Group (RACWG) participating institutions and personnel from both the public and private sectors for their, time, commitment, dedication and efforts which has enabled us to successfully summarize, compile, harmonize and present the results of the terrorism financing risk assessments in a consistent manner, and for producing the Terrorism Financing National Risk Assessment Guidance, 2025, to assist all the responsible agencies and institutions, including the private sector to effectively implement the outcomes of TF risk assessments in the country.

CAPT. (RTD.) SAITOTI K. MAIKA, MBS
Director General/Financial Reporting Centre & Coordinator for National ML/TF/PF Risk Assessments

CONTENTS

LIST OF TABLES

1.0 NATIONAL TERRORISM FINANCING RISK

1.1 The National Terrorism Financing (TF) Risk

The residual TF risk for Kenya is assessed as ***Medium High***, while the inherent TF risk is ***High***. The overall sectoral vulnerability to TF, in relation to domestic operations is ***Medium***, while the overall sectoral vulnerability for TF in relation to international operations is ***Medium High***. The national vulnerability against internal TF risk is ***Medium Low***, while the vulnerability against Outgoing, Incoming and Transit TF risks are both assessed as ***Medium***, indicating that Kenya is relatively more vulnerable to international (cross-border) TF risk.

1.2 Assessment of TF Threat

The national active terrorism threat is assessed as ***High***, and is expected to remain constant. This is due to the general increase in the number of terrorist ancillary activities, including attacks and casualties by terrorist organizations and the increase in impact of terrorism in Kenya, over the past three years, according to the Global Terrorism Index 2024. The inherent Internal and Incoming TF threats facing Kenya are both assessed as ***High***, while the Outgoing and Transit TF threats are assessed as ***Medium***.

The terrorist organizations identified to have active links in the country, either through physical presence or operation, are Al-Shabaab (AS), Islamic State in Iraq and the Levant (ISIL) faction in Somalia, the Allied Defence Forces (ADF) in DRC, Ahl al-Sunna wal-Jama'a (ASWJ) in Mozambique and lone actors. The risk assessment also identified the Oromo Liberation Army (OLA), an offshoot of the Oromo Liberation Front (OLF), among the regional organized criminal groups which are posing emerging terrorism financing threat to Kenya. The assessment did not however establish a possible nexus between the domestic organized criminal groups, gazetted under the Prevention of Organized Crimes Act, 2010 and TF.

The active terrorist organizations and persons identified to pose TF threat to Kenya as well as the related TF activities are described in Table 1.

Table 1: Terrorist Organizations and Related TF Activities

Terrorist group	**Area of operation**	**Manifestation of the threat**	**Funding**		
			Raise	**Move/store**	**Use**
Al Shabaab (AS)	Somalia	Cross border attacks on security personnel, critical infrastructure and civilians Radicalization, Recruitment, spread of Propaganda, facilitation activities	Legitimate businesses; smuggling and trading in contra band; extortion; zakat collection; taxation of livestock and agricultural products; kidnapping for ransom	Hawala, cash smuggling, MVTs and financial institutions Investment in cash-intensive businesses (sectors) storage in cash or commodities,	Recruitment, training of fighters and experts, weapons acquisition, facilitation of travel, logistical support, salaries, and execution of attacks.
Islamic State in Iraq and the Levant (ISIL)	*ISIL faction in Puntland Somalia-* Al-Karrar office	online radicalization and recruitment; FTFs, spread of propaganda and facilitation activities	Income from online donations; personal funding; robberies; zakat; smuggling and trading in contra-band, extortion and mutual support from sympathizers.	Transfers through Hawala, cash smuggling, mobile transfers and crypto currency. Trade based money laundering	Recruitment; weapons acquisition; facilitation of travel; logistical support; salaries and execution of attacks
	Islamic State – Central Africa Province (ISCAP) operating in Eastern DRC	online radicalization and recruitment; propaganda and facilitation	Robberies; kidnappings for ransom; trade in natural resources; illegal taxation; protection rackets; donations; arms smuggling /trafficking.	Hawala; MVTS; smuggling routes and black-market trade to facilitate the movement of both money and goods.	Recruitment; weapons acquisition; facilitation of travel; and logistics handling.
	Islamic State in Mozambique (ASWJ) operating in Cabo Delgado Province	online radicalization/ recruitment; and facilitation	receives part of its funds from the ISIL Somalia; ordinary trade; extortion activities; kidnapping for ransom and smuggling of fauna and flora products	Hawala, MVTS and legitimate businesses, Virtual assets	Recruitment, weapons acquisition, facilitation of travel and logistical support

Lone Actors	Local affiliates to either AS or ISIL	Radicalization/ recruitment, Attacks	own income, donations, crowdfunding and other criminal activities.	MVTs and Hawala	Logistical support
Organized criminal groups (analysed to determine any links to TF)	*Domestic organized criminal groups*- limited to groups Gazetted under the Prevention of Organized Crimes Act, 2010.	No link found between these criminal groups' activities with TF. However, the groups are at risk of being infiltrated and exploited by terror groups given that their motive is financial gain.	Funding by the political class; extortion of the public; drug trafficking; arms trafficking; racketeering; smuggling of goods and humans; human trafficking and donations	Cash, mobile money, MRPs	Purchase of firearms, sustaining operations and investment.
	Cross-border organized criminal groups- Oromo Liberation Front/ Army (OLF-OLA)	Intelligence sources show that OLF-OLA and AS jointly kidnapped two foreigners in Northern Kenya, in August 2024, indicating links international TF	criminal activities; arms, narcotics & human trafficking; kidnapping for ransom; illegal mining ; crowdfunding; contraband trade along the porous Kenya-Ethiopian border	Cash smuggling	To sustain their activities; salaries; purchase of weapons

The domestic TF threat posed by the presence of terrorist organizations in Kenya is assessed as ***High*** and expected to remain constant. This is informed by the activities of these groups in relation to their high level of funding needs to sustain their activities, possibility of raising funds within Kenya and funds transfer activities through formal and informal channels. The incoming and outgoing cross-border TF threats posed by the groups are assessed as ***High*** and ***Medium*** respectively, and are expected to persist. Despite some of the groups like the ISCAP and ASWJ having negligible presence in the country, they still pose a significant TF threat due to transfer and movement of funds through Kenya from their other financial bases, as well as involvement as foreign terrorist fighters (FTFs).

1.3 Other Factors Contributing to the Assessment of TF Threat

I. Sympathizers

Kenya has large populations residing along the expansive porous border with Somalia, some of whom may be supportive to terrorist organizations, persons and ideology. Some of them engage in trade of contraband goods and smuggling, facilitate funds transfer through Hawala and registered money remittance services on behalf of terrorists, harbour terrorists, provide safe passage and assist in funding logistics for their operations thus posing a TF threat. This situation is worsened by the presence of large refugee complexes in the North Eastern region of Kenya.

The domestic TF threat posed by sympathizers is assessed as ***Medium*** and is expected to remain constant. The outgoing cross-border TF threat posed by sympathizers is also considered as ***Medium***, and is expected to remain constant.

II. Neighbors

Kenya shares an expansive porous border with Somalia thus facilitating illicit trade and flow of funds. Further, Kenya is geographically positioned within a conflict prone region contributing to the influx of refugees and other undocumented immigrants into Kenya providing grounds for recruitment and facilitation activities or spill-over effect to Kenya.

Countries Posing Significant TF Threat to Kenya

Country	Foreign Inward TF threat
Somalia	High
South Africa	High
Mozambique	High
UAE	Medium
Tanzania	Medium
Uganda	Medium
DRC	Medium
North America	Medium

Other Countries Exposure to TF from Kenya

Country	Foreign Outward TF threat
DRC	High
Mozambique	High
Somalia	High
Uganda	Medium
Rwanda	Medium
Tanzania	Medium

IV. Finance and Trade Hub Function of the Jurisdiction

Kenya's strategic geographical positioning coupled with its strong technological, industrial and economic base, makes it an anchor State. A well-developed financial, payment, and transport systems inadvertently provide opportunities for terrorist groups to collect, transfer, store and use funds through obscured methods, thus exacerbating cross-border TF for Kenya.

V. Strategic Goods and Services.

In Kenya, strategic goods[1] and services and dual use goods are defined in the pending Strategic Goods Control Bill, 2024. But the trade in strategic goods still require special approval as provided for under various legislations. As it stands currently, there are no business entities or NPOs that provide strategic goods and services in areas with active terrorist threat in Kenya.

1.4 Assessment of TF Vulnerability

The level of national TF vulnerability stems from the gaps and weaknesses in the national measures for the prevention and detection of TF and the enforcement of CFT measures in the country. Based on the assessment, the overall national vulnerability to TF is assessed as ***Medium***, while the national combating ability (mitigating control) is ***Medium Low***.

The national TF vulnerability was established through in-depth analysis involving:

i. *Strengths and weaknesses in the country's CFT regime*, such as adequacy of legislation and institutional frameworks; quality of CFT policies, and strategies; effectiveness of customs controls on cash and similar instruments; effectiveness of border controls on strategic goods; effectiveness of immigration controls; and the effectiveness of the targeted financial sanctions regime.

ii. *Contextual factors*, like the quality of FIU intelligence gathering and processing; capacity and resources for TF investigations, prosecutions and judicial processes (including asset forfeiture); integrity and independence of financial crime investigators, prosecutors and judges (including asset forfeiture); and the effectiveness of domestic as well as international cooperation.

iii. *Mechanisms for effective implementation of CFT control measures*, including supervision and remediation. That is, the level of formalization of the economy (low levels imply low regulatory and law enforcement capability, limited economic regulations – thriving unregistered businesses, significant tax crimes, among others); availability of reliable identification infrastructure; availability of independent information sources; and the availability and access to beneficial ownership information.

[1] Strategic goods means military goods, dual use-goods, weapons of mass destruction and their means of delivery and nationally controlled goods and includes any component used in their production, means of delivery and their related service

2.0 TERRORISM FINANCING RISKS AT THE SECTORAL LEVEL

The TF risks borne by financial and DNFBP sectors contribute to the national TF risks. FATF recommends consideration and understanding of TF risks posed to specific sectors in the jurisdiction, based on materiality, TF awareness and geographic reach. The 2022 Mutual Evaluation Report (MER) indicated that the vulnerabilities associated with Hawala activities, cross border currency movements, and relatively weak NPOs regulation framework heighten the TF risks for the country.

The following factors contributed significantly in determining the level of TF risks at the sectoral level:

2.1 Inherent TF Threat Assessment at Sectoral Level

2.1.1 Existence of typologies

This involved review and consideration of cases related to abuse of a particular sector for TF domestically or globally. The focus was placed on the identified terrorist entities and their networks, funds, sources, destination, methods, and channels of financing.

2.1.2 Geographical factors

Involved analysing the significance of geographic factors which the sector is exposed to that affect the TF threat. All aspects of physical, social and economic geography were analysed. For example, the exposure that could arise from business activities or branches of business entities in areas with active terrorist threats.

2.1.3 Demographic factors

Involved analysing the significance of demographic factors to which the sector is exposed that affect inherent TF threat. For example, exposure may arise from the client base through designated entities and persons, affiliation with an active terrorist threat, or persons who may be sympathetic to terrorist persons or ideology.

2.1.4 Other inherent threat factors

The importance of the other threat factors related to TF in each sector was determined. For example, inherent TF threat may arise from exploitation of natural resources if terrorist entities have control. The presence of large refugee community in the country also present additional inherent TF threat.

2.2 Inherent TF Vulnerability Assessment at Sectoral Level

2.2.1 Size of the sector relative to other sectors

The overall size (or turnover) of the sector compared with the other sectors being assessed was necessary considering that it is possibly easier to conceal TF related transactions within relatively large sectors (through comingling, disguising, among others).

2.2.2 Magnitude and nature of international transactions

This involved analysis of the level of (*i*) outward international transactions or operations, (including transactions to high-risk geographical locations from business entities in a particular sector), and (*ii*) inward international transactions or operations, (including transactions from high-risk geographical locations to business entities in a particular sector). The assumption is that the higher the level of international transactions or operations, especially to/from high risk jurisdictions, the higher the level of exposure to the sector.

2.2.3 Client base profile

This inherent vulnerability indicator involved conducting client base profile to determine the level of exposure resulting from the client base of service providers in a particular sector.

2.2.4 Level of cash activity

The higher the level of cash activity within a particular sector the higher the TF exposure.

2.2.5 Level of intermediation

The level of use of agents, vendors, and other intermediaries in each sector was determined.

2.2.6 Ease of abuse (utility) for TF

The utility of each particular sector to TF was analysed. For example, (*i*) whether services and products offered by a particular sector permit person-to-person fund transfers that allow quick movement of funds to higher-risk locations, (*ii*) possibility of transactions in which reliable and comprehensive information on the originator and beneficiary information of (cross-border) fund transfers may be lacking, among others. These are key factors that may endear a particular sector to TF abuse i.e., be more easily exploited (vulnerable) to TF.

2.3 TF Risks Mitigating Controls at the Sectoral Level

TF mitigating controls include measures that are mandatory within the CTF legal and structural regime as well as other practices adopted by both the public and private sectors to mitigate inherent TF risk. These include the institutional, legal, regulatory, supervisory, asset forfeiture and judicial frameworks that govern public sector actions through specific obligations. Also, the internal control measures and systems adopted by the reporting institutions (private sector) to reduce TF risks.

2.3.1 Legislative improvements

The 2024 Post Observation Progress Report for Kenya acknowledged the significant improvements to the country's CFT legal and institutional frameworks. Kenya enacted the Anti-Money Laundering and Combating of Terrorism Financing Laws (Amendment) Act, 2023 to provide for TF/PF preventative measures. Additionally, the Proceeds of Crime and Anti-Money Laundering Regulations, 2023 and the Prevention of Terrorism (Implementation of the United Nations Security Council Resolutions on the Prevention, Suppression and Disruption of Proliferation Financing) Regulations, 2023, were enacted to address the TF/PF Technical Compliance issues identified in the 2022 MER.

While the legislative improvements have generally promoted the CFT measures in the country, the implementation of targeted financial sanctions (TFS) related to TF, provided for under Recommendation 6 still has outstanding technical compliance gaps.

2.3.2 CFT obligations

The obligations set under the Kenya's CFT regime corroborate international best practice, thus provide strong control against TF in the country. These include the mandatory requirement for all eligible entities to:

i. register with the FRC as reporting institutions;
ii. undertake a risk assessment to enable identification, assessment, understanding, monitoring, management and mitigation the risks associated with TF. And then development and implementation of policies, controls and procedures for effective management and mitigation of the identified risks;
iii. monitor and report suspicious activities and transactions;
iv. verify customer identity;

v. establish and maintain customer records;
vi. stablish and maintain internal reporting procedures;
vii. prevent the use of new technologies for terrorism financing, among others.

2.3.3 Supervision and enforcement

All financial sector regulators are carrying our thorough prudential and market conduct regulations, including enforcing entry and licensing requirements. For CFT regulation, the landscape is uneven with the supervisor for banks and MVTS having separate units for AML/CFT regulation, hence well developed. For the other non-bank supervisors, CFT regulation is combined with prudential and market conduct regulation, hence moderately effective. For DNFBPs, CFT regulation is majorly conducted by FRC due to inadequate capacity from respective supervisors.

Generally, the level of CFT supervision in Kenya is fair. All the CFT regulators have sufficient powers and resources to administer sanctions and penalties for CFT breaches. The CFT regulators' oversight and supervision generally span both offsite and onsite activities. The CFT offsite supervision and monitoring involve among others, ongoing desk-based review, regular interactions with supervised entities, among others. On-site activities involve performing full scope, targeted or thematic CFT on-site inspections, the frequency and intrusiveness of which is determined by the scope.

Effective supervision and enforcement also enhance implementation of know your employee principle. For instance, banks and MVTS are required to notify the regulator before onbording money laundering reporting officer (MLRO). All reporting entities must notify the FRC when MLRO is on-boarded or when replaced. Additionally, reporting entities are required to notify respective regulators when changes occur in senior management, including Board of Directors. These measures are significant for reasonable CFT supervision and regulation for quality control against unscrupulous staff.

2.3.4 Sensitization and awareness creation

Financial institutions have largely embedded TF capacity building requirement within the institutional internal control mechanisms. For banks and MVTS, the trainings are tailored for specific categories of staff depending on the assigned roles and are continuous. However, the implementation levels are significantly varied within the financial sector, and minimal within the DNFBP sector.

The financial sector regulators have also increased outreach and other engagement with the reporting institutions, including through feedback mechanisms, sensitization and TF-related trainings. This has been achieved through development and issuance of sector-specific Guidance, TF red-flag indicators and sharing typology reports. However, these initiatives have largely benefited reporting institutions within the financial sector. For the DNFBPs, very little outreach has been extended so far.

2.3.5 Measures undertaken by reporting institutions

i. ***Risk assessment*** - financial institutions, especially commercial banks, micro-finance banks and MVTS, have generally taken appropriate steps to identify, assess and understand their institutional TF risks, including for customers, countries or geographic areas, products, services, transactions or delivery channels. Risk assessments are fairly documented, kept up-to-date, and relevant risk factors are considered before determining the level of overall risk and the appropriate level and type of mitigation required. Banks and MVTS normally assess the TF risks of new products and business practices (including new distribution mechanisms and the use of new or developing technologies for both new and pre-existing products). When required, the risk assessment information is provided to competent authorities.

ii. ***Customer due diligence (CDD)*** – most financial institutions normally complete CDD requirements when onboarding clients. CDD measures conducted include identifying and verifying client's identity using reliable, independent source documents and data; identifying the beneficial owner and obtaining information on the purpose and intended nature of the business relationship as well as the source of wealth; screening against politically exposed persons (PEPs), sanctions lists and other high-risk lists; performing enhanced due diligence (EDD) where TF risks are higher, for instance, regarding business relationships and transactions with natural and legal persons from higher risk countries and is typically also used for clients such as PEPs; seeking senior management approval before establishing relatively risky business relationships.

iii. ***Access to beneficial ownership (BO) information*** – reporting institutions are developing and maintaining respective BO information. Also to strengthen the country's BO framework, the Business Registration Service (BRS) developed a centralized electronic register for BO information in October 2020, which provides for timely access to the BO information by competent authorities. Further, legal amendments are underway to also grant access to the e-register by reporting institutions for AML/CFT purposes, especially to facilitate the CDD/EDD procedures like verification of BO information of customers, especially of high risk clients like PEPs. These steps have been taken to improve the effectiveness of implementation of AML/CFT control measures in the country.

iv. ***Transaction monitoring and reporting*** - the use of off-the-shelf transaction monitoring programs are very common across the financial sector. Inspection reports show that several reporting institutions are adopting range of scenario-based profiles, business rules, parameters and alerts to detect suspicious activity. Following detection, institutional internal policies require unusual transactions to be escalated and EDD to be completed where appropriate. The information collected are then used for reporting and to update customer risk profiles.

The transaction monitoring framework has however, experienced some implementation challenges. These include difficulties in transaction monitoring of institutional or corporate customers due to the large variety of transactional profiles and small numbers of clients and transactions; challenges in building customer profiles for effective monitoring of transactions involving one-off customers, non-uniform transaction monitoring standards by different reporting institutions, ineffective or non-existent transaction monitoring by some institutions, especially DNFBPs.

v. ***Institutional internal controls*** – the financial institutions in Kenya have internal policies, controls and procedures to effectively mitigate and manage TF risks albeit in varying degrees based on type of institution. Banks and MVTS generally have stronger internal control measures relative to the other non-bank financial institutions. These typically include defining TF risk indicators that are approved by the Board of Directors, communicated to the staff, and monitored on a regular basis. The controls also include documenting key policies and procedures (e.g. in relation to CDD; client risk assessment; transaction monitoring; wire transfers; correspondent banking; new technologies; reliance on third parties; foreign branches and subsidiaries; reporting of suspicious transactions; and tipping off.

2.4 Sectoral Overview

The TF sectoral risk assessment focused on the following institutions: Banks (both commercial and microfinance), Money Value Transfer Services (MVTS), Digital Credit Providers (DCPs), Designated Non-Financial Business and Professionals (DNFBPs), Non-Profit Organizations (NPOs), SACCOs, Insurance and Securities.

The sectors were selected based on: (i) materiality and relevance to Kenya's TF risk context; (ii) existence and prevalence of typologies relating to TF abuse; and (iii) FATF guidance on TF risk assessment, TF awareness and the geographic reach. Other sectors including, casino, lawyers, accountants and company service providers were assessed to pose relatively very low TF risk in the country.

In addition to the sectors listed above, Kenya conducted separate TF risk assessments for Legal Persons and Trusts, and Virtual Assets (VA) and Virtual Assets Service Providers (VASPs) in 2023. Regarding legal persons and arrangements TF risks, private limited companies and trusts were assessed to have ***Medium Low*** risk. The other legal persons (structures), including foreign companies, public limited companies, limited liability partnerships, unlimited companies and companies limited by guarantee, were assessed as posing ***Low*** TF risks. Legal structures which are likely to be abused for TF purposes are falling within logistics (transport), real estate, trade, and energy (oil marketing) industries. The *case examples* 9, 10 and 11, clearly demonstrate how legal structures can be abused for TF in Kenya.

Regarding virtual assets (VA) and virtual assets service providers' (VASPs) TF risks, the overall TF risk was rated as ***Medium Low***. The report show that the use of VAs and VASPs are more prevalent among the younger population, mostly aged between 18 and 40 years, who rely on VAs for investment and speculation purposes. Majority of VA customers use peer-to-peer (P2P) mechanism to facilitate exchange from fiat to virtual and vice versa. Moreover, the TF threat posed by P2P VA transfer services was rated ***High***. *Case example* 11 demonstrates emerging typology regarding abuse of VAs and VASPs for TF, as it relates to Kenya.

2.5 Banking Sector

The banking sector in Kenya comprises 39 commercial banks and 14 microfinance banks, all of which are licensed and overseen by the Central Bank of Kenya. The TF risk for the banking sector is assessed as ***Medium High***, resulting from the TF threat rating of ***High*** and TF vulnerability rating of ***Medium***. The quality of the instituted CFT control measures are assessed as ***Medium Low***.

Table 2: Nature of TF Risks in Banking Sector

Risk Type	Description of Inherent Risk	Emerging Trends
Use of bank accounts for TF	-Terror groups exploiting personal, business, and charity-linked accounts to receive and move TF-related funds. -Small-value structured deposits to avoid detection thresholds. -Residual CDD/KYC loopholes.	Increased use of multiple accounts and digital banking platforms to facilitate TF.
Correspondent banking services	-Cross-border wire transfers and offshore banking to layer and move TF funds *(re: Case 6 & 7)* -Weak CFT oversight in high-risk jurisdictions making tracing transactions difficult. -Exposure to regional TF risks from conflict zones *(re: Case 1 & 2)*	-Offering of correspondent banking services to high risk jurisdictions of DRC and Somalia
Trade-related transactions	-Banks facilitate trade transactions that terrorist financiers may use to mask or layer the purpose of money movements. -Complex trade transactions and weak customs oversight make it difficult to monitor movement and purpose of payments *(re: case 10)*	Rise in use of shell companies and abuse of trade finance to disguise TF-financing as legitimate transactions.
Abuse of PBOs & charitable organizations	-Terror-linked NPOs use banks to store and distribute funds under the disguise of humanitarian assistance. -Cash-intensive operations make it hard to track fund origins. -Abuse of international donor funded programs	Digital fundraising and online crowdfunding replacing traditional PBO-based TF mechanisms *(re: Case 4)*

Table 3: TF Vulnerability Posed by Banking

Vulnerability	Description	Impact
Beneficial ownership transparency	- Difficulty in verification of BO information in relation to trusts making it difficult to trace individuals behind high-risk transactions. - Terrorist financiers exploiting companies to hide their identities.	- Increased layering and integration of TF-linked funds through banks. - Difficulty in identifying and freezing TF-linked assets.
Oversight of correspondent banking	- Weak CFT monitoring of offshore accounts and international financial institutions in CFT deficient jurisdictions. - Banks facilitating cross-border wire transfers and correspondent banking with high-risk jurisdictions *(re: Case 6 & 7)*	- Exposure to international TF networks. - Risk of de-risking by global banks, limiting access to foreign markets.
Structured transactions	- Terror financiers using multiple small-value transactions across multiple accounts to avoid detection. - Business transactions structured to avoid detection as TF linked arrangements *(re: Case 15)* - Banking loopholes in monitoring low-value transactions allowing TF layering.	- Difficulty in tracking and linking funds to terrorist networks. - Higher risk of regulatory non-compliance for banks.

2.6 Money Value Transfer Service (MVTS) Sector

According to the FATF, "money or value transfer services (MVTS) refer to financial services that involve the acceptance of cash, cheques, other monetary instruments or other stores of value and the payment of a corresponding sum in cash or other form to a beneficiary by means of a communication, message, transfer, or through a clearing network to which the MVTS provider belongs. The 2024 TF National Risk Assessment conceived the MVTS sector to include MRPs, MNOs and forex bureaus.

The major TF threat factors facing the MVTS sector in Kenya include:

i. MVTS branches operating in high-risk jurisdictions;
ii. Reliance on third parties such as agents and international money transfer (IMT) partners who may fail to adhere to the CFT measures thus present opportunities for illicit actors to raise/ move funds for TF;
iii. Heightened border transactions due to trading activities of Kenya and its neighbors, some of which face political instability;
iv. Transactions are rapid hence inadequate due diligence procedures can be exploited by persons to facilitate TF; and
v. Identity theft i.e., use of borrowed/stolen identification cards to perpetuate TF activities.

2.6.1 Money Network Operators (MNOs)

Mobile Network Operators (MNOs) in Kenya, are licensed by the Communication Authority of Kenya (CAK). Licensed MNOs intending to provide payments and other financial services are required to apply for licensing from Central Bank of Kenya (CBK) where they are issued with a payment service provider (PSP) license. Currently, there are four MNOs licensed to operate in Kenya. The TF threat, vulnerability and overall TF risks posed by MNOs in the country are all rated ***High***.

MNO products are accessible by subscribers irrespective of the jurisdictional boundaries which increases the vulnerability. They can be exploited for crowd funding thereby collecting funds and facilitating subsequent transfers to terrorist organizations. The transactions are non-face-to-face; thus terrorist persons or sympathizers may register account(s) with non-authentic identification documents for purposes of TF.

2.6.2 Money Remittance Providers (MRPs)

Money Remittance Providers (MRPs) are entities that receive instructions from customers to transfer money or value across borders to foreign recipients. The TF threat, vulnerability and overall TF risks posed by MRPs are all assessed as ***High***.

MRPs offer fast and relatively low-cost methods of transferring funds across borders making them vulnerable for TF. The delivery channels for MRPs to customers, including in-person, phone, bank, and third-party arrangements are increasing TF vulnerability, since they facilitate access by sympathizers to send and remit funds to and from high-risk jurisdictions. Further, the MRP subsector is exposed to TF where product delivery arrangements are outsourced. These include the use of partners and third-party service providers to fulfil transactions without proper KYC/CDD in foreign jurisdictions.

Case no. 6 shows how funds from ISIL in Somalia were moved to South Africa then eventually to Mozambique through Kenya using an international MRP and Hawala.

2.6.3 Forex Bureaus

Foreign exchange bureau or Forex bureau or Bureau de change is an entity licensed under the Central Bank of Kenya Act to transact foreign exchange business, which is the buying and selling of foreign currencies. The TF risks posed by forex bureaus is assessed as ***Medium High.*** The TF threat level is rated ***Low***, while the vulnerability is also ***Medium High***.

Forex Bureaus only transact in hard cash hence identifying and verifying the source of these funds can be difficult, making them susceptible for facilitation of conversion to preferred currencies by sympathizers. Most forex bureaus have lean structures, low capital and are family owned. Due to these salient features, basic CFT controls are rarely adopted by forex bureaus. Additionally, CFT measures, including delivery of sufficient CFT training to staff, are not adequate.

Some of the bureaus experience challenges verifying customers' identity due to lack of systems that are linked to the national identification database. Additionally, most of the customers are walk-in making it difficult to establish a relationship, jeopardizing KYC procedures.

2.7 Digital Credit Providers

Digital credit providers (DCPs) are licensed by CBK principally to provide credit services. Following the Business Laws (Amendment) Act, 2024, these credit service providers are now referred to as non-deposit taking credit providers. The TF risk posed by the DCP sub-sector is assessed as ***Low***. Both the TF threat and vulnerability are also rated ***Low***.

The TF risks manifestation through DCPs can be in the form of access to loans for TF purposes, ownership of DCP businesses by individuals linked to terrorists or terrorist sympathizers, and provision of capital for DCP business activities from terrorist funds.

2.8 Non-Profit Organizations (NPOs)

FATF conceives an NPO to cover, "a legal person or arrangement or organization that primarily engages in raising or disbursing funds for purposes such as charitable, religious, cultural, educational, social or fraternal purposes, or for the carrying out of other types of "good works."

The overall TF risk posed by NPOs in Kenya is rated ***Medium Low*****.** The overall TF threat for the sector is rated ***Medium*****,** while the vulnerability is rated as ***Medium Low***.

Table 4 indicate the organizations which met the FATF definition of an NPO ('FATF NPOs') and are therefore included within the scope of the assessment.

Table 4: Categorization of FATF NPOs in Kenya

Organization Type	**Rationale for Inclusion**	**FATF NPO**
Non-governmental organizations (NGOs)	All entities registered with the NGO Board meet the FATF definition of NPO, as they are defined as public benefit organizations by the NGO Coordination Act.	Yes
International (foreign) NGOs	All entities registered with the NGOs Board meet the FATF definition of NPO, as they are defined as public benefit organizations by the NGO Coordination Act.	Yes
Community based organizations (CBOs)	Public-benefit CBOs meet the FATF definition as they are established for 'good works'. Mutual-benefit organizations are not established for 'good works' and do not meet the FATF definition.	Partial
Companies limited by guarantee (CLG)	The subset of CLGs established for non-profit, public benefit purposes meet the FATF definition of NPOs.	Yes
Faith based organizations under the Societies Act	Trade unions and professional associations registered under the Societies Act do not meet the FATF definition, as mutual-benefit groups are not established for "good works.	Partial
Public benefit trusts engaged in fundraising	Only public benefit trusts engaged in fundraising meet the FATF definition of NPO. Non-public benefit or non-fundraising public benefit trusts do not meet the FATF definition	Partial

2.8.1 Nature of the TF threat for NPOs

The report identified Al-Shabaab as posing the greatest TF threat to NPOs in Kenya. The threat was especially high for NPOs working along the Kenya-Somalia border or coastal regions, as well as those in close proximity to terrorist groups or individuals sympathetic to terrorist causes.

There was absence of direct evidence of terrorism financing abuse of NPOs in Kenya. Four possible mechanisms for terrorism financing abuse of NPOs were identified as follows:

i. Abuse of NPOs to raise funds to support terrorist groups and operations.
ii. Abuse of NPOs to conceal the movement or distribution of terrorist funds.
iii. Diversion of legitimate NPO resources to terrorism actors, either intentionally, unintentionally, or under duress.
iv. Development of an operational relationship with an NPO or individuals with an NPO.

2.8.2 Vulnerability of NPOs to TF in Kenya

Inherent TF vulnerabilities that may expose NPOs to TF abuse are as follows:

i. NPOs operating in or near areas with active terrorist presence.
ii. NPOs working with, or in places where there may be, individuals that are sympathetic or supportive of terrorism causes.
iii. NPOs engaged in activities which may bring them into contact with terrorist groups or supporters.
iv. NPOs with unverified or unverifiable funding sources.
v. NPOs with high risk and/or foreign funding sources
vi. NPOs without adequate financial controls or the ability to verify their own activities.
vii. NPOs with unverified partners.
viii. Faith-based NPOs that fall under i and ii above.

2.9 Designated Non-Financial Business and Professions (DNFBPs)

The designated non-financial business and professions (DNFBPs) include, real estate dealers, casinos, lawyers, accountants, trusts and company service providers (TCSPs) and dealers in precious metals and stones (DPMS). The TF risks posed by real estate sector is ***Medium Low***, while DPMS sector poses ***Low*** TF risk in the country.

Table 5: Nature of risk for real estate and Dealers in precious metals and stones

Sector	Risk Level	Risk Manifestation	Reason for the Risk Level
Real estate	*Medium low*	-Collecting rent and using it for TF -Commingling with diaspora remittances -Storage of TF funds in real estate through proxies	-Intensive nature of the sector -Low enforcement level of criminal sanctions -Low CFT awareness and understanding in the sector -Limited KYC during onboarding -Lack of client screening against UN sanction lists -Unlicensed and unregistered real estate agents -Exploitation of the sector for storage, holding and investment of terrorist-related funds
DPMS	*Low*		-Porous borders and political instability within regions that exacerbate TF threat - Smuggling of precious stones and metals -High presence of unlicensed dealers -Extensive use of Cash -Lack of effective and comprehensive regulation -Lack of KYC and CDD of customers

2.10 SACCO Sector

SACCOs are licensed and regulated by the SACCOs Societies Regulatory Authority (SASRA). The overall TF risk posed is assessed as ***Low***. The TF threat to the sector is ***Medium Low,*** while TF vulnerability of the sector is also ***Low***.

SACCOs rely on partnerships and agreements with commercial banks, payment service providers and other third-party fin-techs to access the national payment and settlement infrastructure. SACCOs are therefore not directly exposed to TF risks. Where effective CFT compliance is not adhered to by respective third parties, SACCO services may be compromised and used to aid raising and storage of terrorism financing funds without detection.

2.11 Insurance Sector

The insurance sector is regulated by the Insurance Regulatory Authority. The overall TF risk borne by the insurance sector is assessed as ***Low***. The possible TF threat factors facing the insurance sector include, the possibility of funding terrorism using proceeds from life and investment related insurance policies and offering insurance cover to assets that belong to terrorists. Other threat factors include purchase of insurance products by clients residing in high-risk jurisdictions, investment in life insurance products by terrorists and their associates. However, typologies related to the abuse of life insurance products and services are limited globally, and none exist in Kenya.

2.12 Securities Sector

The sector is regulated by the Capital Markets Authority. The overall TF risk posed is assessed as ***Medium Low***. The TF threat for the sector is assessed as ***Medium,*** while the TF vulnerability for the sector is assessed as ***Low***. The low TF risk rating is attributed to lack of outward and inward international transactions with high- risk TF jurisdictions. Majority of the intermediaries conduct KYC during on-boarding to ensure identity verification, sanctions screening of customers and beneficial owners against UN sanctions lists and conduct enhanced due diligence (EDD) on high-risk customers such as politically exposed persons and high-risk businesses. Additionally, the sector is non-cash based and is fairly regulated.

TF threat factors facing the securities sector include possible investments by front companies that may be set up by terrorist actors to pass out as legal entities. Another threat in the sector could present itself in form of the use of cooperate vehicles for investment by individuals who want to store/hold TF-related funds. Such investments may originate from high-risk jurisdictions which are prone to terrorism as well as civil unrest.

3.0 EMERGING TERRORISM FINANCING RISKS

3.1 Facilitation of Foreign Terrorist Fighters

Foreign Terrorist Fighters (FTFs) are individuals who travel to foreign countries to join or support terrorist organizations. Self-funding by individuals and funding by recruitment/facilitation networks are identified as the two most common methods used to raise funds for FTFs. By virtue of its geographical position, Kenya is vulnerable as a facilitating country and transit country for FTFs. In some instances, Kenya has been exploited by terrorist organizations to move FTFs to jihadi theatres, mostly in Somalia, DRC, Mozambique, Syria.

Other than the evolving patterns of FTFs facilitation, emerging trends further point towards diversifications of both the fighters themselves, and funds related to them, as far as destinations and origins are concerned.

3.2 Abuse of Legal Structures for TF

Legal structures could be increasingly abused for TF purposes, especially those falling within logistics (transport), real estate, trade, and energy sectors. Instances of logistics and freight companies that deal in transportation of oil related products in Kenya, Sudan, Uganda, Rwanda, Burundi, and the rest of East Africa, have been linked with clandestine funds transfer schemes to ADF and IS through logistical support and facilitation or as fronts for raising, laundering, and transferring funds for TF purposes, and have also adopted new technology like virtual assets.

3.3 Use of Sympathizers, Proxies and/or Mules

Reports show that storage and investment of TF related funds are possibly being conducted through pseudo-identities, facilitated by proxies, mules and sympathizers. Kenya's geographical location, large presence of the refugee community and the advanced financial systems with a wide range of financial products have heightened the risk of terrorism and TF activities as well as the possibility of Kenya serving as a transit hub for terror and terrorism financing actors. Current trends indicate that financial institutions located within/in close proximity to the refugee camps, areas close to the Kenya-Somalia border are the most susceptible to such abuse.

3.4 Abuse of Social Media Platforms

Terrorists have embraced the use of social media platforms such as Facebook, WhatsApp, TikTok, YouTube and Telegram for radicalization, recruitment, communication, crowdfunding, planning, facilitation of foreign terrorist fighters (FTFs), training, coordination of attacks and spreading propaganda, among others. In Kenya, crowd-funding through social media is manifesting itself as an emerging TF threat enabling the raising of money from donations or investments from multiple individuals.

3.5 Use of Virtual Assets

The emergence and rapid use of VAs in Kenya presents a new platform for terrorist outfits to conduct financial transactions. This is aided by the inherent features of Vas, especially those relating to anonymity/pseudonymity, cross-border nature and high speed of transfer, which present major challenges to law enforcement authorities to investigate, trace and seize such assets. The listed inherent features make it possible for raising, movement and storage of funds meant for TF with minimal chances of tracing the source and purpose of funds.

3.6 Use of Internet Payment Systems and Prepaid Cards

Internet-based payment services allow customers to access pre-funded accounts via the internet, allowing the transfer of electronic money to others with accounts at the same provider which presents the risk of facilitating illegal activities, such as funding terrorism. Payment methods, like prepaid cards especially open-loop cards are more vulnerable to misuse for illegal fund transfers, including terrorism financing. Kenya has not registered any case of TF via internet payment systems and prepaid cards, since such prepaid cards are linked to specific bank accounts, making transactions traceable through mobile banking or cash deposits, thus offering a layer of monitoring and control.

3.7 Lifting of the Arms Embargo on Somalia

The United Nations Security Council adopted Resolution 2714 on 1st December 2023, lifting the three-decade arms embargo on Somalia, allowing the delivery of weapons, ammunition and military equipment to Somalia. Lifting of this embargo is projected to increase AS access to weapons, owing to the high level of corruption reported on the Somali government as well as the significant influence wielded by AS within Somalia. The use of the additional weapons is likely to sustain or escalate the ongoing terrorist attacks castigated by AS in Kenya, especially the regions closer to the border with Somalia. The acquired weapons are also likely to be used to escalate other TF ancillary activities, including kidnapping for ransom, arms smuggling, among others.

APPENDICES: TF RELATED CASE TYPOLOGIES

Appendix 1: Banking case examples

Case example 1: Taxation of smuggled contraband
Reports have described sugar as 'the most smuggled good' into Kenya, accounting for almost half of all recorded smuggling instances. The sugar that finds its way across the Kenyan border is typically smuggled from Kismayo. Smuggling into Kenya is facilitated by the refugee complexes in North Eastern Kenya, that is the vast Dadaab, Dagahaley, Hagardera and Ifo refugee camps in Dadaab sub-county of Garissa County. Refugees in the camps have established links with their relatives back in Somalia, who bring in imported goods such as sugar from Kismayu Port in Southern Somalia. Investigations reveal that illegal immigrants smuggle the goods through the porous border with Somalia, all of which are taxed by AS in transit from the Somalia side.

Case example 2: Illegal taxation of livestock
Communities residing in the NE region of Kenya depend on pastoralism as an economic activity, and consequently take part in livestock trade. During the dry seasons the communities migrate into Somalia in search of water and pastures, and usually end up paying zakat and protection fees to the Al Shabaab. The communities also trade their livestock, and one of the largest livestock trading markets is in Garissa. Livestock brokers facilitate cross-border trading of the livestock along the Somalia-Kenya trade corridor and as such livestock from Somalia also find their way into the market. The Garissa livestock market also provides an opportunity for brokers who might be sourcing livestock to sell to the Somalia side. All the livestock from and into the Somalia side are taxed. UN reports indicate that throughout the Somalia routes, illicit taxation rates range between $16 per head for camels, $8 per head of cattle, and $2 per head of goat. This thus providing funds to AS.

Case example 3: Mwok Anwar, the Kulbiyow lead attacker
Mwok Anwar ventured into business, selling imported second-hand wares including mobile phones in Eastleigh, where he was believed to have been radicalized. He grew his business and ventured into the transport business. Reports indicate that the capital was from family inheritance. He eventually developed residential property from his investments. With his new-found wealth, he was also becoming heavily influential and even set up a make-shift mosque where he led a break-away faction of the Muslim community in Umoja. It is believed that Mwok helped radicalize dozens of young men from poor households, who envied his business acumen. He then left for Somalia, leaving his business and properties under his mother's care. Reports suggest that the mother sent money from the businesses to Mwok in Somalia, on several occasions, to support his activities. Mwok was onboard a VBIED used in the Kulbiyow attack against a KDF camp in 2017, where he also died.

Case example 4: IS cells in Kenya
Around 2016, IS group recruiters used social media platforms like Facebook, Whatsapp and Instagram, for recruiting and crowd-funding, eventually facilitating travel of recruits from Kenya to Libya through different routes in Africa. The cells mostly targeted bright university students. Case in point is that of two young medical doctors Farah Dagane and Hiish Ahmed, who travelled to Libya to join IS through Kampala and Khartoum, and started recruiting individuals from Kenya, using the same platforms and crowdfunding. Investigations revealed that IS relied on a human trafficking ring called the Magafe network with agents in Kenya to facilitate the transport of recruits from Kenya to Libya. Ali Hussein Ali, arrested in 2016, was the link for the network in Kenya, and also facilitated the movement of money through various countries before reaching Libya to conceal transaction trails. On arrival in Libya, the recruits and illegal immigrants were detained by the Magafe network and would be released on payment of between Sh250,000 and Sh700,000 which is later transferred through Hawala in Kenya to Mogadishu and later to IS.

Case example 5: Dusit attack financing
Evidence showed how MAA on diverse dates between 14th October 2018 and 12th January 2019 while using his mobile phone numbers 0****** and 07******* as well as telephone number 07******* (belonging to his deceased brother, IAA) sent KES 836, 900 to Ali Salim Gichunge alias Farouk (the main attacker/terrorist) to facilitate the terrorist attack at Dusit Hotel while utilizing telephone number 07****** registered to EKM using a stolen ID.

Case example 6: The case of XYZ and ABC illicit transfer networks
The first confirmed transfer from the Islamic State to ISCAP (DRC) came via Kenyan Islamic State facilitator XYZ in late 2017. Together with ABC – a woman who had planned to travel with XYZ's father to Syria as his fiancée but was arrested before she left and later released – XYZ directed money being moved through a financial network that spanned Europe, America, the Middle East, and Africa. They were initially able to avoid detection by transferring the money through a personal account connected to a family business and through the Hawala system, but both XYZ and ABC were eventually arrested in July 2018. In total, the pair moved over $150,000 to Islamic State affiliates in Central Africa, Syria, and Libya.

Further investigations revealed that at least $11,000 of the total funds, were sent to known ISCAP operatives in Uganda. For instance, between October 2017 and January 2018, the facilitator received 8 Western Union (WU) transactions in Mombasa, Kenya, totalling to $9,222, from 8 senders in Western Europe, Southern Europe, Africa, and the Middle East. The facilitator sent one $825 transaction in November 2017 from Kenya to South Kivu province in Eastern DRC. South Kivu is the primary base of operations for the Islamic State's affiliate in the DRC, the Allied Democratic Forces (ADF).

The facilitator 's extended Western Union network also included WU activity in Turkey, Afghanistan, Senegal, Belgium, Denmark, Germany, France, Finland, Kosovo, Russia, and Kazakhstan. Nationalities of individuals in the financier's network included Syria, Kenya, Mauritania, Uganda, and other nationalities from Europe, Central Asia, and South Asia.

Case example 7: Transfers by IS network in East Africa through Heeryo Enterprises
In the case of this network, which operated from 2019 to late 2020, much of the money was sent through Hawala networks under the auspices of Heeryo Trading Enterprise, a Somalia- and South Africa-based company. Registered in Johannesburg and with operations in Mogadishu, Heeryo facilitated the movement of hundreds of thousands of dollars from Somalia to South Africa, as well as transfers from South Africa to Kenya for further distribution. Facilitators in Kenya either directly disbursed the funds or, on instructions from Heeryo's manager in Johannesburg, sent them to other money transfer offices where recipients withdrew them. Funds were also sent through a variety of regional Hawala and remittance networks, some of which have branches throughout East Africa, the Middle East, and various Western countries.

Between 2019 and 2020, the network transferred over $400,000 to two Da'esh operatives based in Johannesburg, South Africa, then part of the funds, almost $134,000 to Kenya, from where they were redirected to Uganda, the United Republic of Tanzania and Mozambique. At least $60,000 of the $400,000 originally transferred from Da'esh in Somalia was received by known ADF collaborators in Uganda.

Case example 8: Utilization of funds in the botched Merti VBIED plot
In the foiled 2018 plot, a vehicle had been converted into a vehicle-borne improvised explosive device (VBIED) with assorted weapons (5 Type 56-2 AK-pattern assault rifles, 36 magazines of ammunition, 36 unprimed F1 grenades and their firing pins, 3 knives) and Al Shabaab paraphernalia, including a black flag. Funds were received via two MVTS funds transfers, totalling $15,000 from Kismayo. The funds were used to purchase two vehicles worth about KES 2,100,000. $9,500. Also to pay an arms smuggler for the acquisition and smuggling of the weapons. The funds also catered for costs of hiring a driver, rent expenses of KES 16,000 per month, procurement of fake IDs, purchase of air tickets worth KES 12,000 and other logistical expenses. The operation cost Al-Shabaab less than $50,000 up to the point that it was disrupted by the National Police Service.

Case example 9 – TF funds transiting Kenya
D.F.G, a Kenyan national was reported to be facilitating money transfer from Kenya to Uganda, Tanzania, and Mozambique to individuals linked to ADF and possibly IS. D.F.G was reported to be managing entities that were linked to IS-DRC financial institution. The facilitation is said to be conducted through his employees. Additionally, he was also linked to a logistics and freight company that deals in transportation of oil related products in Kenya, Sudan, Uganda, Rwanda, Burundi, and the rest of East Africa.

Case example 10: Movement of equipment through Kenyan logistical companies
Kenya Defense Forces under AMISOM intercepted a DJI Matrice 350 RTK drone in Dhobley, Somalia. Investigations revealed that SRH, alongside his Kenyan counterparts, imported the drone from South Africa for onward transfer to Somalia through Kenya for the benefit of Al Shabaab. SRH imported the drone under the directions of AY, an operative in Somalia who wired a total of KES1.5 million from Somalia via mobile money, which was subsequently sent to South Africa via Hawala.

The drone was facilitated to the country through the help of logistical companies. Once in the country, the drone was repackaged and sent via a lorry to Dhobley, Somalia. On November 30, 2023, the subject was charged alongside two other suspects with eight counts of terror-related charges including TF, and the acquisition of restricted goods.

Case example 11: TF funds transfer using VASPs
In a recent terrorist financing case under investigation, one AK, a cash courier linked to Allied Defense Forces (ADF), was found to have been remitting money through a virtual assets service provider (VASP) to individuals within East Africa, DRC and Mozambique for terrorism purposes. The source of the money is a Ugandan terror suspect based in South Africa who receives instructions on remittances from the ADF commander in DRC.

Case example 12: TF/PF/ML Financial investigation on the seizure of foreign currency and gold ornaments at JKIA
In October 2022, Customs and Border Control officials within Jomo Kenyatta International Airport (JKIA) seized smuggled cash totalling to US$ 857,300 and gold ornaments, including bangles, neckless, chains and rings, from six (6) alleged Kenyans arriving from Mumbai, India via Addis Ababa, Ethiopia aboard Ethiopian Airways Flight. It is reported the suspicious cash was concealed in hand-carry luggage containing shoes and clothes and were discovered after secondary verification after the x-ray scanners showed images resembling currency. Some of the gold ornaments were worn by the six suspects. The six women had not filled the requisite monetary declaration Forms

Preliminary investigations by ATPU revealed that all the six women are involved in nefarious activities while operating at a common guest house/lodge in Eastleigh, Nairobi.

Case example 13: Cholo Abdi
Cholo Abdi, was indicted by a US court in December 2020 on suspicion that he was sponsored by the AS to attend pilot training in the Philippines with the aim of conducting a 9/11-Style Attack at the Direction of Al Shabaab. Cholo Abdi operated 3 bank accounts all funded through cash deposits in Kenya, between 2017 and 2019 he received a total of USD 30,000.00. All deposits conducted in amounts between USD 2,000 and 5,000 deposits were all conducted after traveling to Kenya. Funds were used to pay for his pilot training fees and upkeep in the Philippines. The funds were utilized through ATM cash withdraws in the Philippines.

Case example 14: Coercion of NPOs operating within AS controlled areas in Somalia and along the border
Based on intelligence report, NPOs with offices in Kenya (registered in Kenya) but operating in Gedo and Jubaland regions in Somalia, where AS has control, are coerced into paying illegal taxes and protection fees to be allowed to operate. Consequently, the collected fees are used to finance AS activities in general.
Terrorists posing as legitimate natural or legal persons or arrangements (other than NPOs) to benefit from NPO programmes or supplying the NPO with goods and services (e.g. security or supplies). The case of Dusit attack where an international NPO was used to facilitate purchase of communication/IT equipment which aided the attack.

Terrorists or their facilitators infiltrating an NPO, for example appearing to work as an ordinary NPO representative/partner, then abuse the NPO's resources through diversion of funds to terrorists, or providing support to their recruitment efforts. The case of Dusit attack where the staff of an NPO was used as conduit to facilitate the purchase of the telecommunication equipment, is an example. Other cases involving aid/relief food.

Case example 15: Lafarge case
Lafarge and LCS executives intentionally structured their agreements with ISIS to compensate the terrorist organization based on the amount of cement that LCS was able to sell – effectively, a revenue-sharing agreement – to incentivize the terrorist group to act in LCS's economic interest. The two terrorist organisations received nearly six million dollars. Larfage and its subsidiary pleaded guilty to providing material support and resources in Northern Syria from 2013 to 2014 to the Islamic State of Iraq and al-Sham (ISIS) and the al-Nusrah Front (ANF), both U.S.-designated foreign terrorist organizations. It was later established that Larfage owns Bamburi cement Company which is listed in the Nairobi Stock Exchange. Fincem Holding Limited and Kencem Holding Limited are subsidiaries of Lafarge Holcim. This gives Lafarge Holcim 58.6% control of Bamburi Cement.

Case example 16 – Terrorists exploit PoEs
One of the Dusit D2 complex attackers is suspected to have crossed the border from Somalia to Kenya through El Wak, a few days before the attack. The same PoE was used to smuggle a vehicle-borne improvised explosive Device (VBIED) which was intercepted by police at Merti, Isiolo County in 2018.

Appendix 2: DNFBPs case examples

Case example 1: Taxation of smuggled contraband
Reports have described sugar as 'the most smuggled good' into Kenya, accounting for almost half of all recorded smuggling instances. The sugar that finds its way across the Kenyan border is typically smuggled from Kismayo. Smuggling into Kenya is facilitated by the refugee complexes in North Eastern Kenya, that is the vast Dadaab, Dagahaley, Hagardera and Ifo refugee camps in Dadaab sub-county of Garissa County. Refugees in the camps have established links with their relatives back in Somalia, who bring in imported goods such as sugar from Kismayu Port in Southern Somalia. Investigations reveal that illegal immigrants smuggle the goods through the porous border with Somalia, all of which are taxed by AS in transit from the Somalia side.

Case example 2: Illegal taxation of livestock
Communities residing in the NE region of Kenya depend on pastoralism as an economic activity, and consequently take part in livestock trade. During the dry seasons the communities migrate into Somalia in search of water and pastures, and usually end up paying zakat and protection fees to the Al Shabaab. The communities also trade their livestock, and one of the largest livestock trading markets is in Garissa. Livestock brokers facilitate cross-border trading of the livestock along the Somalia-Kenya trade corridor and as such livestock from Somalia also find their way into the market. The Garissa livestock market also provides an opportunity for brokers who might be sourcing livestock to sell to the Somalia side. All the livestock from and into the Somalia side are taxed. UN reports indicate that throughout the Somalia routes, illicit taxation rates range between $16 per head for camels, $8 per head of cattle, and $2 per head of goat. This thus providing funds to AS.

Case example 3: Mwok Anwar, the Kulbiyow lead attacker
Mwok Anwar ventured into business, selling imported second-hand wares including mobile phones in Eastleigh, where he was believed to have been radicalized. He grew his business and ventured into the transport business. Reports indicate that the capital was from family inheritance. He eventually developed residential property from his investments. With his new-found wealth, he was also becoming heavily influential and even set up a make-shift mosque where he led a break-away faction of the Muslim community in Umoja. It is believed that Mwok helped radicalize dozens of young men from poor households, who envied his business acumen. He then left for Somalia, leaving his business and properties under his mother's care. Reports suggest that the mother sent money from the businesses to Mwok in Somalia, on several occasions, to support his activities. Mwok was onboard a VBIED used in the Kulbiyow attack against a KDF camp in 2017, where he also died.

Case example 4: IS cells in Kenya
Around 2016, IS group recruiters used social media platforms like Facebook, Whatsapp and Instagram, for recruiting and crowd-funding, eventually facilitating travel of recruits from Kenya to Libya through different routes in Africa. The cells mostly targeted bright university students. Case in point is that of two young medical doctors Farah Dagane and Hiish Ahmed, who travelled to Libya to join IS through Kampala and Khartoum, and started recruiting individuals from Kenya, using the same platforms and crowdfunding. Investigations revealed that IS relied on a human trafficking ring called the Magafe network with agents in Kenya to facilitate the transport of recruits from Kenya to Libya. Ali Hussein Ali, arrested in 2016, was the link for the network in Kenya, and also facilitated the movement of money through various countries before reaching Libya to conceal transaction trails. On arrival in Libya, the recruits and illegal immigrants were detained by the Magafe network and would be released on payment of between Sh250,000 and Sh700,000 which is later transferred through Hawala in Kenya to Mogadishu and later to IS.

Case example 5: Dusit attack financing
Evidence showed how MAA on diverse dates between 14th October 2018 and 12th January 2019 while using his mobile phone numbers 0****** and 07******* as well as telephone number 07******* (belonging to his deceased brother, IAA) sent KES 836, 900 to Ali Salim Gichunge alias Farouk (the main attacker/terrorist) to facilitate the terrorist attack at Dusit Hotel while utilizing telephone number 07****** registered to EKM using a stolen ID.

Case example 6: The case of XYZ and ABC illicit transfer networks
The first confirmed transfer from the Islamic State to ISCAP (DRC) came via Kenyan Islamic State facilitator XYZ in late 2017. Together with ABC – a woman who had planned to travel with XYZ's father to Syria as his fiancée but was arrested before she left and later released – XYZ directed money being moved through a financial network that spanned Europe, America, the Middle East, and Africa. They were initially able to avoid detection by transferring the money through a personal account connected to a family business and through the Hawala system, but both XYZ and ABC were eventually arrested in July 2018. In total, the pair moved over $150,000 to Islamic State affiliates in Central Africa, Syria, and Libya.

Further investigations revealed that at least $11,000 of the total funds, were sent to known ISCAP operatives in Uganda. For instance, between October 2017 and January 2018, the facilitator received 8 Western Union (WU) transactions in Mombasa, Kenya, totalling to $9,222, from 8 senders in Western Europe, Southern Europe, Africa, and the Middle East. The facilitator sent one $825 transaction in November 2017 from Kenya to South Kivu province in Eastern DRC. South Kivu is the primary base of operations for the Islamic State's affiliate in the DRC, the Allied Democratic Forces (ADF).

The facilitator 's extended Western Union network also included WU activity in Turkey, Afghanistan, Senegal, Belgium, Denmark, Germany, France, Finland, Kosovo, Russia, and Kazakhstan. Nationalities of individuals in the financier's network included Syria, Kenya, Mauritania, Uganda, and other nationalities from Europe, Central Asia, and South Asia.

Case example 7: Transfers by IS network in East Africa through Heeryo Enterprises
In the case of this network, which operated from 2019 to late 2020, much of the money was sent through Hawala networks under the auspices of Heeryo Trading Enterprise, a Somalia- and South Africa-based company. Registered in Johannesburg and with operations in Mogadishu, Heeryo facilitated the movement of hundreds of thousands of dollars from Somalia to South Africa, as well as transfers from South Africa to Kenya for further distribution. Facilitators in Kenya either directly disbursed the funds or, on instructions from Heeryo's manager in Johannesburg, sent them to other money transfer offices where recipients withdrew them. Funds were also sent through a variety of regional Hawala and remittance networks, some of which have branches throughout East Africa, the Middle East, and various Western countries.

Between 2019 and 2020, the network transferred over $400,000 to two Da'esh operatives based in Johannesburg, South Africa, then part of the funds, almost $134,000 to Kenya, from where they were redirected to Uganda, the United Republic of Tanzania and Mozambique. At least $60,000 of the $400,000 originally transferred from Da'esh in Somalia was received by known ADF collaborators in Uganda.

Case example 8: Utilization of funds in the botched Merti VBIED plot

In the foiled 2018 plot, a vehicle had been converted into a vehicle-borne improvised explosive device (VBIED) with assorted weapons (5 Type 56-2 AK-pattern assault rifles, 36 magazines of ammunition, 36 unprimed F1 grenades and their firing pins, 3 knives) and Al Shabaab paraphernalia, including a black flag. Funds were received via two MVTS funds transfers, totalling $15,000 from Kismayo. The funds were used to purchase two vehicles worth about KES 2,100,000. $9,500. Also to pay an arms smuggler for the acquisition and smuggling of the weapons. The funds also catered for costs of hiring a driver, rent expenses of KES 16,000 per month, procurement of fake IDs, purchase of air tickets worth KES 12,000 and other logistical expenses. The operation cost Al-Shabaab less than $50,000 up to the point that it was disrupted by the National Police Service.

Case example 9 – TF funds transiting Kenya

D.F.G, a Kenyan national was reported to be facilitating money transfer from Kenya to Uganda, Tanzania, and Mozambique to individuals linked to ADF and possibly IS. D.F.G was reported to be managing entities that were linked to IS-DRC financial institution. The facilitation is said to be conducted through his employees. Additionally, he was also linked to a logistics and freight company that deals in transportation of oil related products in Kenya, Sudan, Uganda, Rwanda, Burundi, and the rest of East Africa.

Case example 10: Movement of equipment through Kenyan logistical companies

Kenya Defense Forces under AMISOM intercepted a DJI Matrice 350 RTK drone in Dhobley, Somalia. Investigations revealed that SRH, alongside his Kenyan counterparts, imported the drone from South Africa for onward transfer to Somalia through Kenya for the benefit of Al Shabaab. SRH imported the drone under the directions of AY, an operative in Somalia who wired a total of KES1.5 million from Somalia via mobile money, which was subsequently sent to South Africa via Hawala.

The drone was facilitated to the country through the help of logistical companies. Once in the country, the drone was repackaged and sent via a lorry to Dhobley, Somalia. On November 30, 2023, the subject was charged alongside two other suspects with eight counts of terror-related charges including TF, and the acquisition of restricted goods.

Case example 11: TF funds transfer using VASPs

In a recent terrorist financing case under investigation, one AK, a cash courier linked to Allied Defense Forces (ADF), was found to have been remitting money through a virtual assets service provider (VASP) to individuals within East Africa, DRC and Mozambique for terrorism purposes. The source of the money is a Ugandan terror suspect based in South Africa who receives instructions on remittances from the ADF commander in DRC.

Case example 12: TF/PF/ML Financial investigation on the seizure of foreign currency and gold ornaments at JKIA

In October 2022, Customs and Border Control officials within Jomo Kenyatta International Airport (JKIA) seized smuggled cash totalling to US$ 857,300 and gold ornaments, including bangles, neckless, chains and rings, from six (6) alleged Kenyans arriving from Mumbai, India via Addis Ababa, Ethiopia aboard Ethiopian Airways Flight. It is reported the suspicious cash was concealed in hand-carry luggage containing shoes and clothes and were discovered after secondary verification after the x-ray scanners showed images resembling currency. Some of the gold ornaments were worn by the six suspects. The six women had not filled the requisite monetary declaration Forms

Preliminary investigations by ATPU revealed that all the six women are involved in nefarious activities while operating at a common guest house/lodge in Eastleigh, Nairobi.

Case example 13: Cholo Abdi

Cholo Abdi, was indicted by a US court in December 2020 on suspicion that he was sponsored by the AS to attend pilot training in the Philippines with the aim of conducting a 9/11-Style Attack at the Direction of Al Shabaab. Cholo Abdi operated 3 bank accounts all funded through cash deposits in Kenya, between 2017 and 2019 he received a total of USD 30,000.00. All deposits conducted in amounts between USD 2,000 and 5,000 deposits were all conducted after traveling to Kenya. Funds were used to pay for his pilot training fees and upkeep in the Philippines. The funds were utilized through ATM cash withdraws in the Philippines.

Case example 14: Coercion of NPOs operating within AS controlled areas in Somalia and along the border

Based on intelligence report, NPOs with offices in Kenya (registered in Kenya) but operating in Gedo and Jubaland regions in Somalia, where AS has control, are coerced into paying illegal taxes and protection fees to be allowed to operate. Consequently, the collected fees are used to finance AS activities in general.

Terrorists posing as legitimate natural or legal persons or arrangements (other than NPOs) to benefit from NPO programmes or supplying the NPO with goods and services (e.g. security or supplies). The case of Dusit attack where an international NPO was used to facilitate purchase of communication/IT equipment which aided the attack.

Terrorists or their facilitators infiltrating an NPO, for example appearing to work as an ordinary NPO representative/partner, then abuse the NPO’s resources through diversion of funds to terrorists, or providing support to their recruitment efforts. The case of Dusit attack where the staff of an NPO was used as conduit to facilitate the purchase of the telecommunication equipment, is an example. Other cases involving aid/relief food.

Case example 15: Lafarge case

Lafarge and LCS executives intentionally structured their agreements with ISIS to compensate the terrorist organization based on the amount of cement that LCS was able to sell – effectively, a revenue-sharing agreement – to incentivize the terrorist group to act in LCS's economic interest. The two terrorist organisations received nearly six million dollars. Larfage and its subsidiary pleaded guilty to providing material support and resources in Northern Syria from 2013 to 2014 to the Islamic State of Iraq and al-Sham (ISIS) and the al-Nusrah Front (ANF), both U.S.-designated foreign terrorist organizations. It was later established that Larfage owns Bamburi cement Company which is listed in the Nairobi Stock Exchange. Fincem Holding Limited and Kencem Holding Limited are subsidiaries of Lafarge Holcim. This gives Lafarge Holcim 58.6% control of Bamburi Cement.

Case example 16 – Terrorists exploit PoEs

One of the Dusit D2 complex attackers is suspected to have crossed the border from Somalia to Kenya through El Wak, a few days before the attack. The same PoE was used to smuggle a vehicle-borne improvised explosive Device (VBIED) which was intercepted by police at Merti, Isiolo County in 2018.